IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF DELAWARE

SYMBOL TECHNOLOGIES, INC., a Delaware Corporation, and WIRELESS VALLEY COMMUNICATIONS, INC., a Delaware Corporation,

Plaintiffs and Counter-Defendants,

v.

ARUBA NETWORKS, INC., a Delaware Corporation,

Defendant and Counter-Claimant.

C. A. No. 07-519-JJF

DEMAND FOR JURY TRIAL

ARUBA NETWORKS, INC.'S MOTION FOR LEAVE TO AMEND ITS ANSWER AND FOR LEAVE TO SERVE COUNTERCLAIMS ON MOTOROLA, INC.

Pursuant to Federal Rule of Civil Procedure 15 and District of Delaware Local Rule 15.1, Defendant and Counter-Claimant Aruba Networks, Inc. ("Aruba") moves for an order granting leave to file an amended answer and counterclaims against Plaintiffs Symbol Technologies, Inc. ("Symbol") and Wireless Valley, Inc. ("Wireless Valley"). A copy of the proposed amended answer and counterclaims and a copy noting the proposed changes are attached hereto as Exhibit A and Exhibit B respectively. Pursuant to Federal Rules of Civil Procedure 13(h) and 20(a), Aruba also moves for an order granting leave to join Motorola, Inc. ("Motorola") as a counterclaim defendant. In support of its motion, Aruba states as follows:

1. On May 7, 2008 the parties and the Court participated in a Rule 16 status and scheduling conference. The parties thereafter initiated discovery.

2. On May 9, 2008, the Court set a Scheduling Order with deadlines for motions to amend and motions to join other parties of September 2, 2008. (D.I. 37).

3. The discovery cut-off date is January 30, 2009. (D.I. 49).

4. It is well-established that, as to the amendment of pleadings, "leave shall be freely given when justice so requires." Fed. R. Civ. P. 15(a). Under the law of this District, "absent any apparent or declared reason—such as undue delay, bad faith or dilatory motive on the part of the movant, repeated failure to cure deficiencies by amendments previously allowed, undue prejudice to the opposing party by virtue of allowance of the amendment, futility of amendment, etc.—the leave [to amend one's pleadings] should, as rules require, be freely given." *Agere Sys. Guardian Corp. v. Proxim, Inc.*, 190 F. Supp. 2d 726, 732 (D. Del. 2002) (citing *Foman v. Davis*, 371 U.S. 178, 182 (1962)). The Third Circuit has stated that absent a clear reason such as delay, bad faith, or prejudice, it is an abuse of discretion for a district court to deny leave to amend. *See Alvin v. Suzuki*, 227 F.3d 107, 121 (3d Cir. 2000).

5. Plaintiffs will suffer no prejudice from the proposed amendment. The amendment seeks to add two counterclaims for infringement of Aruba patents concerning technology that is very similar to the technology encompassed by Plaintiffs' patents. Aruba seeks leave well within the deadline for amending pleadings set forth by this Court's Scheduling Order. There is ample opportunity for discovery remaining, as the cut-off for fact discovery is not until January 30, 2009 and not a single document has yet been produced in this case. Indeed, the parties are still negotiating a Protective Order.

6. Moreover, there is a large overlap of witnesses and evidence relevant to Plaintiffs' and Aruba's patents; many of the facts will be the same as those asserted in the original pleadings. Similar to Plaintiffs' claims, Aruba's infringement claims relate to wireless network products such as access points, switches and controllers. In fact, the products accused by Aruba include some of the very same products identified Plaintiffs have identified as commercial

embodiments of their patents, and consequently are already at issue in this case. And the inventors on Aruba's patents are the same people that Plaintiffs will need to depose to prosecute their current case against Aruba.

7. Nor can Aruba be accused of delay. The claims are brought promptly after the factual and legal bases for the claims arose—one patent first issued on May 20, 2008, and the other was first acquired by Aruba in March 2008. Finally, the addition of Aruba's infringement counterclaims is expected to make any mediation more productive because issues regarding all parties' intellectual property would be on the table. Therefore, in the interest of justice, Aruba should be permitted to amend its answer and counterclaims.

8. A party may be joined to a lawsuit as a permissive party to a counterclaim under Federal Rule of Civil Procedure 20. Fed. R. Civ. P. 13(h), 20. Rule 20 permits joinder of defendants if "(A) any right to relief is asserted against them jointly, severally, or in the alternative, with respect to or arising out of the same transaction, occurrence, or series of transactions or occurrences; and (B) any question of law or fact common to all defendants will arise in the action." It has been recognized in this District that lawsuits involving patents asserted against multiple defendants warrant joinder. *See, e.g., SRI Int'l, Inc. v. Internet Sec. Sys.*, Civ. NO. 04-1199-SLR, 2005 U.S. Dist. LEXIS 6797, at *10-*12 (D. Del. Apr. 13, 2005) (holding that the Court would be required to hold a Markman hearing to construe the asserted claims, to consider the same prior art, level of ordinary skill, conception date, reduction to practice, etc., and that "[i]t would be an inefficient use of judicial resources for the court to perform all of these tasks twice.").

9. Aruba's right to relief on its counterclaims arises out of a common series of transactions—i.e., Motorola's, Symbol's and Wireless Valley's sales of infringing products.

Additionally, many common questions of law and fact relating to claim construction, validity and infringement will undoubtedly arise in this suit.

10. Moreover, the joinder of Motorola at this time is not prejudicial to Plaintiffs. Aruba will prosecute this case under the current discovery schedule and its limitations. And there is no prejudice to Plaintiffs because Motorola is effectively already in this case—indeed, it has been controlling the case from the outset. Plaintiffs Symbol and Wireless Valley are wholly-owned subsidiaries of Motorola (Complaint at ¶¶ 1-2) (D.I. 1). But it was Motorola who announced this lawsuit in a press release entitled, "Motorola Files a Lawsuit against Aruba Networks for Wireless Patent Infringement" (Declaration of Etai Lahav, Exh. 1 (hereinafter "Lahav Decl., Exh. X")). Additionally, Plaintiffs have requested that Motorola attorneys review confidential information on behalf of Symbol and Wireless Valley (Lahav Decl., Exh. 2) and current Motorola attorneys were substantively involved in the prosecution of both Symbol's and Wireless Valley's patents (Lahav Decl., Exhs. 3-5). Finally, seven out of nine people disclosed in Plaintiffs' Initial Disclosures are Motorola employees, including three out of five of the named inventors on Plaintiffs' patents (Lahav Decl., Exh. 6). Therefore, in the interest of justice and judicial efficiency, Aruba should be permitted to amend its answer and counterclaims to include Motorola as a counterclaim defendant.

11. Pursuant to the attached certification, counsel for Aruba has made a reasonable effort to reach agreement with Plaintiffs' counsel pursuant to District of Delaware Local Rule 7.1.1. The parties were unable to reach agreement.

WHEREFORE, Aruba respectfully requests that the Court grant its motion to file an amended pleading in the form attached hereto as Exhibit A. A form of order is attached hereto.

/s / Frederick L. Cottrell, III
Frederick L. Cottrell, III (#2555)
Richards, Layton & Finger
One Rodney Square
920 North King Street
P. O. Box 551
Wilmington, DE 19899
Telephone: (302) 651-7700

Attorneys for Defendant and Counter-Claimant
ARUBA NETWORKS, INC.

OF COUNSEL:

MATTHEW D. POWERS
WEIL, GOTSHAL & MANGES LLP
Silicon Valley Office
201 Redwood Shores Parkway
Redwood Shores, CA 94065
Telephone: (650) 802-3000

NICHOLAS GROOMBRIDGE
PAUL E. TORCHIA
ETAI LAHAV
WEIL, GOTSHAL & MANGES LLP
New York Office
767 Fifth Avenue
New York, NY 10153-0119
Telephone: (212) 310-8000

Dated: July 16, 2008

CERTIFICATE OF SERVICE

I hereby certify that on July 16, 2008, I electronically filed the foregoing with the Clerk of Court using CM/ECF which will send notification of such filing(s) to the following and which has also been served as noted:

BY HAND

Richard L. Horwitz
David E. Moore
Potter Anderson & Corroon LLP
Hercules Plaza, 6th Floor
1313 N. N. Market Street
Wilmington, DE 19801

I hereby certify that on July 16, 2008 I transmitted the document by Federal Express to the following non-registered participant:

VIA FEDERAL EXPRESS
Eric J. Lobenfeld
Ira J. Schaefer
Lawrence Brocchini
Arun Chandra
Hogan & Hartson L.L.P.
875 Third Avenue
New York, NY 10022

/s/ Frederick L. Cottrell, III
Frederick L. Cottrell, III (#2555)
cottrell@rlf.com

EXHIBIT A

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF DELAWARE

SYMBOL TECHNOLOGIES, INC., a Delaware Corporation, and WIRELESS VALLEY COMMUNICATIONS, INC., a Delaware Corporation,

Plaintiffs,

v.

ARUBA NETWORKS, INC., a Delaware Corporation,

Defendant.

C. A. No. 07-519-JJF

DEMAND FOR JURY TRIAL

ARUBA NETWORKS, INC., a Delaware Corporation

Counter-Claim Plaintiff,

v.

MOTOROLA, INC., a Delaware Corporation, SYMBOL TECHNOLOGIES, INC., a Delaware Corporation, and WIRELESS VALLEY COMMUNICATIONS, INC., a Delaware Corporation,

Counter-Claim Defendants.

ARUBA NETWORKS, INC.'S SECOND AMENDED ANSWER AND COUNTERCLAIMS

PARTIES

1. Aruba admits that in Securities and Exchange Commission filings Motorola, Inc., has described Symbol as a wholly owned subsidiary. Aruba is without knowledge or information sufficient to form a belief as to the truth of the remaining allegations of Paragraph 1 of the Complaint and therefore denies those allegations.

2. Aruba admits that in Securities and Exchange Commission filings Motorola, Inc., has described Wireless Valley as a wholly owned subsidiary. Aruba is without knowledge or information sufficient to form a belief as to the truth of the remaining allegations of Paragraph 2 of the Complaint and therefore denies those allegations.

3. Aruba admits that it is a Delaware corporation with a principal place of business at 1344 Crossman Avenue, Sunnyvale, CA 94089-1113, and that, for purposes of this action, The Corporation Trust Company is its registered agent for service of process in Delaware. The Complaint does not make clear what plaintiffs mean in the third sentence of Paragraph 3 of the Complaint, and Aruba therefore denies those allegations.

JURISDICTION AND VENUE

4. Aruba admits that this action purports to arise under the Patent Laws of the United States, Title 35, United States Code, but denies any wrongdoing or liability. Aruba further admits that this Court has subject matter jurisdiction over the allegations in the Complaint under 28 U.S.C. §§ 1331 and 1338(a).

5. Aruba does not dispute that for purposes of this action venue is proper in this judicial district.

6. Aruba admits that it is subject to personal jurisdiction in this judicial district because Aruba is a Delaware corporation with an agent for service of process in Delaware. Except as expressly admitted, Aruba denies the allegations of Paragraph 6 of the Complaint.

THE ASSERTED PATENTS – DENIAL OF INFRINGEMENT

7. Aruba admits that U.S. Patent No. 7,173,922 ("the '922 patent"), entitled "Multiple Wireless Local Area Networks Occupying Overlapping Physical Spaces," purports to have issued on February 6, 2007, but denies that this patent was duly and legally issued. Aruba admits that a document that purports to be a copy of the '922 patent is attached to the Complaint as Exhibit A, but Aruba lacks knowledge that it is a true and correct copy and therefore denies the remaining allegations of Paragraph 7 of the Complaint.

8. Aruba admits that U.S. Patent No. 7,173,923 ("the '923 patent"), entitled "Security In Multiple Wireless Local Area Networks," purports to have issued on February 6, 2007, but denies that this patent was duly and legally issued. Aruba admits that a document that purports to be a copy of the '923 patent is attached to the Complaint as Exhibit B, but Aruba lacks knowledge that it is a true and correct copy and therefore denies the remaining allegations of Paragraph 8 of the Complaint.

9. Aruba is without knowledge or information sufficient to form a belief as to the truth of the allegations of Paragraph 9 of the Complaint and therefore denies those allegations.

10. Aruba admits that U.S. Patent No. 6,625,454 ("the '454 patent"), entitled "Method and System for Designing or Deploying a Communications Network Which Considers Frequency Dependent Effects," purports to have issued on September 23, 2003, but denies that this patent was duly and legally issued. Aruba admits that a document that purports to be a copy of the '454 patent is attached to the Complaint as Exhibit C, but Aruba lacks knowledge that it is a true and correct copy and therefore denies the remaining allegations of Paragraph 10 of the Complaint.

11. Aruba admits that U.S. Patent No. 6,973,622 ("the '622 patent"), entitled "System and Method for Design, Tracking, Measurement, Prediction and Optimization of Data Communication Networks," purports to have issued on December 6, 2005, but denies that this patent was duly and legally issued. Aruba admits that a document that purports to be a copy of the '622 patent is attached to the Complaint as Exhibit D, but Aruba lacks knowledge that it is a true and correct copy and therefore denies the remaining allegations of Paragraph 11 of the Complaint.

12. Aruba is without knowledge or information sufficient to form a belief as to the truth of the allegations of Paragraph 12 of the Complaint and therefore denies those allegations.

FIRST ASSERTED CLAIM – '922 PATENT

13. Aruba incorporates its responses to the allegations of Paragraphs 1-12 of the Complaint here.

14. Aruba denies the allegations of Paragraph 14 of the Complaint.

15. Aruba denies the allegations of Paragraph 15 of the Complaint.

16. Aruba denies the allegations of Paragraph 16 of the Complaint.

17. Aruba denies the allegations of Paragraph 17 of the Complaint.

18. Aruba denies the allegations of Paragraph 18 of the Complaint.

SECOND ASSERTED CLAIM – ’923 PATENT

19. Aruba incorporates its responses to the allegations of Paragraphs 1-12 of the Complaint here.

20. Aruba denies the allegations of Paragraph 20 of the Complaint.

21. Aruba denies the allegations of Paragraph 21 of the Complaint.

22. Aruba denies the allegations of Paragraph 22 of the Complaint.

23. Aruba denies the allegations of Paragraph 23 of the Complaint.

24. Aruba denies the allegations of Paragraph 24 of the Complaint.

THIRD ASSERTED CLAIM – ’454 PATENT

25. Aruba incorporates its responses to the allegations of Paragraphs 1-12 of the Complaint here.

26. Aruba denies the allegations of Paragraph 26 of the Complaint.

27. Aruba denies the allegations of Paragraph 27 of the Complaint.

28. Aruba denies the allegations of Paragraph 28 of the Complaint.

29. Aruba denies the allegations of Paragraph 29 of the Complaint.

30. Aruba denies the allegations of Paragraph 30 of the Complaint.

FOURTH ASSERTED CLAIM – ’622 PATENT

31. Aruba incorporates its responses to the allegations of Paragraphs 1-12 of the Complaint here.

32. Aruba denies the allegations of Paragraph 32 of the Complaint.

33. Aruba denies the allegations of Paragraph 33 of the Complaint.

34. Aruba denies the allegations of Paragraph 34 of the Complaint.

35. Aruba denies the allegations of Paragraph 35 of the Complaint.

36. Aruba denies the allegations of Paragraph 36 of the Complaint.

SEPARATE DEFENSES

37. In addition to the defenses described below, Aruba expressly reserves the right to allege additional defenses as they become known through the course of discovery.

FIRST DEFENSE – NON-INFRINGEMENT

38. Aruba has not infringed, directly or indirectly, any valid asserted claim of the ’922, ’923, ’454, or ’622 patents (collectively “patents-in-suit”).

SECOND DEFENSE – INVALIDITY UNDER §§ 102 AND 103

39. Aruba is informed and believes, and on that basis alleges, that each of asserted claims of each of the patents-in-suit is invalid for failure to meet the conditions of patentability set forth in 35 U.S.C. §§ 102 and 103, because the alleged inventions thereof are anticipated by, taught by, suggested by, and/or obvious in view of the prior art, and no claim of any of the patents-in-suit can be validly construed to cover any Aruba product or method.

THIRD DEFENSE – INVALIDITY UNDER § 112

40. Aruba is informed and believes, and on that basis alleges, that each of the asserted claims of each of the patents-in-suit are invalid for failure to comply with 35 U.S.C. § 112.

FOURTH DEFENSE – INVALIDITY UNDER § 101

41. Aruba is informed and believes, and on that basis alleges, that each of the asserted process claims of each of the patents-in-suit are invalid for failure to comply with 35 U.S.C. § 101.

FIFTH DEFENSE – EQUITABLE ESTOPPEL

42. The relief sought by Symbol is barred in whole or in part by the doctrine of equitable estoppel.

43. Without limiting the generality of the above allegations, Symbol asserts infringement because “Aruba designs, manufactures, and sells in the United States wireless switches (which it calls mobility controllers), access points, management servers, and related

software for use in connection with WLANs, as well as software for designing, planning, configuring, monitoring, managing, and optimizing WLANs." (Complaint ¶ 3.)

44. Symbol has known this since at least early 2003, when it told Aruba that it (Symbol) wanted to purchase Aruba and spent months trying to convince Aruba to allow Symbol to purchase it. In the course of those efforts, Symbol sent senior engineers – ***including the individual named as the inventor on the '922 and '923 patents-in-suit*** – to Aruba to learn, in copious detail, about Aruba's products. Those discussions lasted for several months. During them, Aruba provided Symbol with extensive access to information about Aruba's products, the way they were designed and built, the way they worked, Aruba's plans for manufacturing and selling them, and Aruba's plans for future products.

45. Although Symbol was very interested in acquiring Aruba and its technologies, ultimately the parties were not able to agree on the complete terms of a transaction.

46. At the time that Symbol was trying to convince Aruba to be purchased, Symbol's '922 and '923 patent applications were no longer confidential – they had been published two years earlier, in 2001. Although those Symbol patent applications were no longer confidential, at no point during Symbol's efforts to convince Aruba did Symbol advise or suggest that if Aruba did not agree to a transaction, Symbol would later assert those pending patents against it. At no point during Symbol's efforts to convince Aruba did Symbol advise or suggest that Symbol had already invented the technology that Aruba had. In fact, quite the contrary: Symbol was very impressed with Aruba's technologies, and told Aruba that it (Symbol) thought those technologies to be superior to, and different from, Symbol's.

47. Symbol's failures and omissions were particularly egregious given that the putative named inventor on those patent applications was an integral part of the senior engineering team that was handpicked by Symbol to learn about Aruba's products – the products that Symbol now says infringes the '922 and '923 patents, and have (according to Symbol) done so since 2003.

48. Symbol’s failures and omissions led Aruba reasonably to infer that Symbol did not intend to enforce any patent rights, including the then-pending ’922 and ’923 patent applications if they issued as patents, against Aruba. As far as Aruba understood from Symbol’s conduct and silence, the parties were going to go compete in the market and let the marketplace decide which technologies and businesses were superior.

49. Since its discussions with Symbol ended in 2003, Aruba has successfully continued its efforts to invest and to innovate. It has established customer relationships based on the products that it disclosed to Symbol during the discussions in 2003. It has spent tens of millions of dollars growing its business based on the products that it disclosed to Symbol in 2003. It has attracted key executive, engineering, finance, and sales personnel based on the success of the products that it disclosed to Symbol in 2003. In these and other ways, it would materially prejudice Aruba for Symbol to be allowed to proceed with its claims.

SIXTH DEFENSE – LACHES

50. The relief sought by Symbol and Wireless Valley is barred in whole or in part by the doctrine of laches. Aruba incorporates the allegations of Paragraphs 43 through 49 here.

51. Without limiting the generality of the above allegations, as noted above, Symbol and Wireless Valley assert infringement because “Aruba designs, manufactures, and sells in the United States wireless switches (which it calls mobility controllers), access points, management servers, and related software for use in connection with WLANs, as well as software for designing, planning, configuring, monitoring, managing, and optimizing WLANs.” (Complaint ¶ 3.) Even leaving aside the 2003 discussions between Symbol and Aruba, Symbol and Wireless Valley have known of Aruba and its activities for years.

52. In May 2003, for example, industry press reported, in an article that quotes both Aruba and Symbol officials, that “Start-ups and old timers in the networking and wireless worlds are flocking to the wireless switching market. The list includes . . . Aruba Wireless Networks, . . . Symbol Technologies, [and others].” There are many other such press and other such examples. Accordingly, Symbol and Wireless Valley knew or reasonably should have known of

the activities now alleged by Symbol and Wireless Valley to infringe the patents-in-suit long ago.

53. In fact, this is true ***even according to Symbol and Wireless Valley***. In an August 2007 industry article about this lawsuit, Symbol's current General Counsel is described as stating that "[a]ll of Aruba's WLAN switch, site planning and radio-frequency management and monitoring products infringe the patents, ***and they have since the company began selling its first products.***" Nevertheless, Symbol and Wireless Valley delayed in bringing this suit until August 2007, on patents that first started issuing in September 2003 – waiting while Aruba invested tens of millions of dollars in designing and testing its products, developing customer relationships, and building its business. Symbol's and Wireless Valley's delay was unreasonable, inexcusable, and prejudicial to Aruba, and Symbol's and Wireless Valley's claims are barred as a result.

SEVENTH DEFENSE – INEQUITABLE CONDUCT ('922 AND '923 PATENTS)

54. Aruba is informed and believes, and on that basis alleges, that individuals charged with a duty of candor on behalf of Symbol failed, with an intent to deceive, to properly disclose to the U.S. Patent and Trademark Office information material to the patentablity of the '922 and '923 patents and failed to follow the requirements of the Manual of Patent Examiners Procedure necessary to have this information considered by the U.S. Patent and Trademark Office.

55. This information includes, but is not limited to, the existence of co-pending U.S. application no. 09/457,624 (the "'624 application"), filed on December 8, 1999. At the time of filing, the '624 application was purportedly owned by Proxim, Inc., and described and claimed subject matter that, to a reasonable patent examiner, would have been material to the patentability of the '922 and '923 patents. On or before October 1, 2004, Proxim assigned its rights in the '624 application to Symbol, so Symbol had knowledge of the contents of the '624 application at least as of the date of the assignment and likely before that. Despite knowing of the highly material contents of the '624 application, individuals charged with a duty of candor on behalf of Symbol failed to disclose the existence of the '624 application to the patent examiner

responsible for the examination of the applications that resulted in the ’922 and ’923 patents. The patent examiner responsible for those applications would have found the 624 application material because, among other things, the examiner would have then been able to determine whether to issue a provisional obviousness-type double patenting rejection.

56. In light of the above, the ’922 and ’923 patents are not enforceable due to inequitable conduct.

EIGHTH DEFENSE – INEQUITABLE CONDUCT (’454 PATENT)

57. Aruba is informed and believes, and on that basis alleges, that individuals charged with a duty of candor on behalf of Wireless Valley failed, with an intent to deceive, to properly disclose to the U.S. Patent and Trademark Office information material to the patentablity of the ’454 patent and failed to follow the requirements of the Manual of Patent Examiners Procedure necessary to have this information considered by the U.S. Patent and Trademark Office.

58. This information includes, but is not limited to, the following: (i) information and publications relating to SMT Plus, a software tool developed, at least in part, by Theodore Rappaport and Roger Skidmore, and licensed to over twenty entities more than one year prior to the filing date of the ’454 patent; (ii) the following publications, which the named inventors and/or prosecuting patent attorneys knew were never considered by the U.S. Patent and Trademark Office due to Wireless Valley’s late submission of an Information Disclosure Statement in violation of U.S. Patent and Trademark Office rules: R.P. Torres, et al., *CINDOOR: An Engineering Tool for Planning and Design of Wireless Systems in Enclosed Spaces*, IEEE Antennas and Propagation Magazine, Vol. 41, No. 4 (Aug. 1999); M. Panjwani et al., *Interactive Computation of Coverage Regions for Wireless Communication in Multifloored Indoor Environments*, IEEE Journal on Selected Areas in Communications, Vol. 14, No. 3 (Apr. 1996); U.S. Patent No. 5,491,644; R. Skidmore et al., *A Comprehensive In-Building and Microcellular Wireless Communication System Design Tool*, The Bradley Department of Electrical Engineering, MPRG-TR-97-13 (Jun. 1997); U.S. Patent No. 5,987,328; Robert Morrow et al., *Getting In*, Wireless Review, Vol. 17, No. 5 (Mar. 1, 2000); (iii) S. Fortune, et al.,

WISE Design of Indoor Wireless Systems: Practical Computation and Optimization, IEEE Computational Science & Engineering, at pp. 58-68 (Spring, 1995), at pp. 58-68 (mentioned in the background section of U.S. Patent No. 7,055,107, another Rappaport and Skidmore patent filed just days before the filing date of the ‘454 patent by the same attorneys that filed the ‘454 patent); and (iv) the following additional publications authored, at least in part, by Theodore Rappaport: Theodore Rappaport et al., *Curriculum Innovation for Simulation and Design of Wireless Communications Systems*, ASEE Annual Conference Proceedings (1996); Keith Blankenship et al., *Measurements and Simulation of Radio Frequency Impulsive Noise in Hospitals and Clinics*, Proceedings of the 47th IEEE Vehicular Technology (1997); Donna Krizman et al., *Modeling and Simulation of Narrowband Phase from the Wideband Channel Impulse Response*, Proceedings of the 47th IEEE Vehicular Technology (1997); Hanif Sherali et al., *Optimal Location of Transmitters for Micro-Cellular Radio Communication System Design*, IEEE Journal on Selected Areas in Communications, Vol. 14, No. 4 (May 1996); Lynn Abbott et al., *Interactive Computation of Coverage Regions for Indoor Wireless Communication*, Proceedings of SPIE - The International Society for Optical Engineering (1995); Jorgen Andersen et al., *Propagation Measurements and Models for Wireless Communications Channels*, IEEE Communications Magazine, Vol. 33, No. 1 (Jan. 1995); M. Panjwani et al., *An Interactive System for Visualizing Wireless Communication Coverage within Buildings*, Wireless Personal Communications, Virginia Tech's 4th Symposium (June 1-3, 1994); and Theodore Rappaport, *Sponsored Research in Radio Propagation and System Design Final Report* (Sep. 26th, 1997).

59. Aruba is informed and believes, and on that basis alleges, that individuals charged with a duty of candor on behalf of Wireless Valley failed, with an intent to deceive, to disclose to the U.S. Patent and Trademark Office the SitePlanner 3.0 product and 1998 manual describing that product. On information and belief, Wireless Valley offered for sale and sold this product and published this manual at least two years before the '454 patent was filed. Wireless Valley has stated in motion papers filed before the Court that the SitePlanner 3.0 product is "in all

material respects the same" as a later version of the same product, SitePlanner 3.16, that Wireless Valley recognized was material and attempted, unsuccessfully, to disclose to the Patent Office. Two of the three inventors of the '454 patent were listed on the SitePlanner 3.0 manual. In addition, on information and belief, the representatives of Wireless Valley who attempted to disclose the SitePlanner 3.16 product to the Patent Office knew about the SitePlanner 3.0 product and product manual. All of these individuals knew or should have known that the 3.0 product and product manual were material to patentability, and, on information and belief, withheld them from the patent office with intent to deceive.

60. In light of the above, the ’454 patent is not enforceable due to inequitable conduct.

NINTH DEFENSE – INEQUITABLE CONDUCT (’622 PATENT)

61. Aruba is informed and believes, and on that basis alleges, that individuals charged with a duty of candor on behalf of Wireless Valley failed, with an intent to deceive, to properly disclose to the U.S. Patent and Trademark Office information material to the patentablity of the ’622 patent and failed to follow the requirements of the Manual of Patent Examining Procedure necessary to have this information considered by the U.S. Patent and Trademark Office, and made false and misleading statements to the U.S. Patent and Trademark Office during the prosecution of the ’622 patent.

62. This information includes, but is not limited to, U.S. Patent No. 6,505,045 (the “’045 patent”). At the relevant time, the Manual of Patent Examining Procedure stated that “It is desirable to avoid the submission of long lists of documents if it can be avoided. Eliminate clearly irrelevant and marginally pertinent cumulative information. ***If a long list is submitted, highlight those documents which*** have been specifically brought to applicant's attention and/or ***are known to be of most significance.***” Despite the highly material disclosure of the ’045 patent, individuals charged with a duty of candor on behalf of Wireless Valley cited the reference by including it as reference number 98 in an Information Disclosure Statement that included a long list of many complex separate documents, all submitted at the same time, to increase the

chance that the ’045 patent would be overlooked by the patent examiner, and stated that the ’045 patent was “only cited as constituting related art of which the applicant is aware” and specifically disclaimed that “the references are relevant or material to the claims.”

63. Aruba is informed and believes, and on that basis alleges, that individuals charged with a duty of candor on behalf of Wireless Valley failed, with an intent to deceive, to disclose to the U.S. Patent and Trademark Office the SitePlanner 3.0 product and 1998 manual describing that product. On information and belief, Wireless Valley offered for sale and sold this product and published this manual at least two years before the earliest possible priority date for any claim of the '622 patent. Wireless Valley has stated in motion papers filed before the Court that the SitePlanner 3.0 product is "in all material respects the same" as a later version of the same product, SitePlanner 3.16, that Wireless Valley recognized was material and attempted to disclose to the Patent Office. Wireless Valley failed to provide a complete copy of the 3.16 manual to the Patent Office, however, but instead excised numerous pages of the document that contain information that the examiner would have found material to patentability of the claims. Two of the three inventors of the '622 patent were listed on the SitePlanner 3.0 manual. In addition, on information and belief, the representatives of Wireless Valley who provided the excerpts of the SitePlanner 3.16 manual to the Patent Office knew about the SitePlanner 3.0 product and product manual. All of these individuals knew or should have known that the 3.0 product and product manual were material to patentability, and, on information and belief, withheld them from the Patent Office with intent to deceive.

64. In light of the above, the ’622 patent is not enforceable due to inequitable conduct.

TENTH DEFENSE – UNCLEAN HANDS

65. Aruba incorporates the allegations of Paragraphs 42 through 64 here.

66. By reason of the acts alleged above, as incorporated, each of Symbol and Wireless Valley are barred from recovery for any asserted infringement of the patents-in-suit by the equitable doctrine of unclean hands.

ELEVENTH DEFENSE – PROSECUTION HISTORY ESTOPPEL

67. Symbol and Wireless are estopped from construing the asserted claims of the patents-in-suit to read on Symbol's products or processes by reasons of statements made to the U.S. Patent and Trademark Office during the prosecution of the applications that led to the issuance of the patents-in-suit.

TWELFTH DEFENSE – PLAINTIFFS' FAILURE TO GIVE NOTICE

68. To the extent Symbol and Wireless Valley seek damages for alleged infringement prior to its giving actual or constructive notice of the patents-in-suit patent to Aruba, the relief they seek is barred by 35 U.S.C. § 287.

DEMAND FOR A JURY TRIAL

69. Aruba requests a trial by jury on all issues so triable.

DENIAL OF PLAINTIFFS' PRAYER FOR RELIEF

70. Aruba denies that Symbol or Wireless Valley are entitled to an award of any relief at all or the relief sought in their prayer for relief against Aruba. Aruba has not infringed, directly, indirectly, contributorily or by inducement, literally or equivalently, willfully or otherwise, any of the asserted claims of the patents-in-suit. Symbol's and Wireless Valley's prayer should be denied its entirety and with prejudice, and Symbol and Wireless Valley should take nothing.

COUNTERCLAIMS

THE PARTIES

71. Aruba is a corporation organized under the laws of the State of Delaware with its principal place of business at 1322 Crossman Avenue, Sunnyvale, California 94089-1113. Aruba was founded in 2002 and went public in 2007. Aruba delivers an enterprise mobility solution that enables secure access to data, voice and video applications across wireless and wireline enterprise networks. It has won many, many awards for its technology innovations.

72. According to the Complaint, Symbol is a corporation organized under the laws of the State of Delaware, with its principal place of business at One Motorola Plaza, Holtsville New

York 11742-1300. According to filings with the U.S. Securities and Exchanges Commission, Symbol is a wholly-owned subsidiary of global behemoth Motorola, Inc., and was acquired by Motorola in September 2006.

73. According to the Complaint, Wireless Valley is a corporation organized under the laws of the State of Delaware with its principal place of business at 4515 Seton Center Parkway, Suite 300, Austin, Texas 78759. According to filings with the U.S. Securities and Exchanges Commission, Wireless Valley is a wholly-owned subsidiary of global behemoth Motorola, Inc., and was acquired by Motorola in December 2005.

74. On information and belief, Motorola, Inc. is a corporation organized under the laws of the State of Delaware with its principal place of business at 1303 East Algonquin Road, Schaumburg, Illinois 60196.

75. On information and belief Motorola, Symbol, and Wireless Valley design, manufacture, and sell in the United States wireless switches, access points and other components for use in connection with WLANs, as well as software for monitoring, and managing WLANs.

JURISDICTION AND VENUE

76. This Court has subject-matter jurisdiction over Aruba’s patent counterclaims, which arise under the patent laws of the United States, pursuant to 28 U.S.C. §§ 1331, 1338, 2201, and 2202.

77. This Court has personal jurisdiction over Symbol, at least because Symbol filed its Complaint for patent infringement in this Court, in response to which these counterclaims are filed. Personal jurisdiction is also proper in this Court because, upon information and belief, Symbol, among other things, places its infringing products in the stream of commerce, which stream is directed at this district.

78. This Court has personal jurisdiction over Wireless Valley, at least because Wireless Valley filed its Complaint for patent infringement in this Court, in response to which these counterclaims are filed. Personal jurisdiction is also proper in this Court because, upon

information and belief, Wireless Valley, among other things, places its infringing products in the stream of commerce, which stream is directed at this district.

79. This Court has personal jurisdiction over Motorola, Inc., because Motorola is a Delaware corporation with an agent for service of process in Delaware. Personal jurisdiction is also proper in this Court because, upon information and belief, Motorola, among other things, places its infringing products in the stream of commerce, which stream is directed at this district.

80. Venue is established in this district for Motorola, Symbol and Wireless Valley pursuant to 28 U.S.C. § 1391 and 1400. Venue is also established in this Court for Symbol and Wireless Valley because they have consented to the propriety of venue in this Court by filing their respective claims for patent infringement in this Court, in response to which Aruba files these counterclaims.

COUNT 1

DECLARATORY JUDGMENT OF NON-INFRINGEMENT

(’922 AND ’923 PATENTS)

81. Aruba incorporates Paragraphs 1 through 68 and 71 through 80 here.

82. An actual and justiciable controversy exists between Aruba and Symbol with respect to the asserted claims of the ’922 and ’923 patents because Symbol has brought this action against Aruba alleging that Aruba infringes claims of the ’922 and ’923 patents, which allegation Aruba denies. Absent a declaration of noninfringement, Symbol will continue wrongfully to assert claims of the ’922 and ’923 patents against Aruba, and thereby cause Aruba irreparable injury and damage.

83. Aruba has not infringed, and does not infringe, the asserted claims of the ’922 or ’923 patents, either directly or indirectly, literally or under the doctrine of equivalents, willfully, or otherwise, and Aruba is entitled to a declaration to that effect.

COUNT 2

DECLARATORY JUDGMENT OF INVALIDITY

(’922 AND ’923 PATENTS)

84. Aruba incorporates Paragraphs 1 through 68 and 71 through 83 here.

85. An actual and justiciable controversy exists between Aruba and Symbol with respect to the asserted claims of the ’922 and ’923 patents because Symbol has brought this action against Aruba alleging that the asserted claims of the ’922 and ’923 patents are valid, which allegation Aruba denies. Absent a declaration of invalidity, Symbol will continue wrongfully to assert claims of the ’922 and ’923 patents against Aruba, and thereby cause Aruba irreparable injury and damage.

86. The ’922 and ’923 patents are invalid for failure to comply with the requirements of Title 35, United States Code, including but not limited to §§ 101, 102, 103, and/or 112, and Aruba is entitled to a declaration to that effect.

COUNT 3

DECLARATORY JUDGMENT OF UNENFORCEABILITY

(’922 AND ’923 PATENTS)

87. Aruba incorporates Paragraphs 1 through 68 and 71 through 86 here.

88. An actual and justiciable controversy exists between Aruba and Symbol with respect to the asserted claims of the ’922 and ’923 patents because Symbol has brought this action against Aruba alleging that the asserted claims of the ’922 and ’923 patents are enforceable, which allegation Aruba denies. Absent a declaration of unenforceability, Symbol will continue wrongfully to assert claims of the ’922 and ’923 patents against Aruba, and thereby cause Aruba irreparable injury and damage.

89. As set forth above, one or more people substantively involved in the prosecution of the application leading to the ’922 and ’923 patents were aware of information material to the patentability of the claims of the ’922 and ’923 patents, but withheld that information from the

U.S. Patent and Trademark Office with the intent to deceive, during the prosecution of the ’922 and ’923 patents.

90. In light of the above, the ’922 and ’923 patents are not enforceable due to inequitable conduct.

COUNT 4

DECLARATORY JUDGMENT OF NON-INFRINGEMENT

(’454 AND ’622 PATENTS)

91. Aruba incorporates Paragraphs 1 through 68 and 71 through 90 here.

92. An actual and justiciable controversy exists between Aruba and Wireless Valley with respect to the asserted claims of the ’454 and ’622 patents because Wireless Valley has brought this action against Aruba alleging that Aruba infringes claims of the ’454 and ’622 patents, which allegation Aruba denies. Absent a declaration of noninfringement, Wireless Valley will continue wrongfully to assert claims of the ’454 and ’622 patents against Aruba, and thereby cause Aruba irreparable injury and damage.

93. Aruba has not infringed, and does not infringe, the asserted claims of the ’454 and ’622 patents, either directly or indirectly, literally or under the doctrine of equivalents, willfully, or otherwise, and Aruba is entitled to a declaration to that effect.

COUNT 5

DECLARATORY JUDGMENT OF INVALIDITY

(’454 AND ’622 PATENTS)

94. Aruba incorporates Paragraphs 1 through 68 and 71 through 91 here.

95. An actual and justiciable controversy exists between Aruba and Wireless Valley with respect to the asserted claims of the ’454 and ’622 patents because Wireless Valley has brought this action against Aruba alleging that the asserted claims of the ’454 and ’622 patents are valid, which allegation Aruba denies. Absent a declaration of invalidity, Wireless Valley will continue wrongfully to assert claims of the ’454 and ’622 patents against Aruba, and thereby cause Aruba irreparable injury and damage.

96. The ’454 and ’622 patents are invalid for failure to comply with the requirements of Title 35, United States Code, including but not limited to §§ 101, 102, 103, and/or 112, and Aruba is entitled to a declaration to that effect.

COUNT 6

DECLARATORY JUDGMENT OF UNENFORCEABILITY

(’454 AND ’622 PATENTS)

97. Aruba incorporates Paragraphs 1 through 68 and 71 through 96 here.

98. An actual and justiciable controversy exists between Aruba and Wireless Valley with respect to the asserted claims of the ’454 and ’622 patents because Wireless Valley has brought this action against Aruba alleging that the asserted claims of the ’454 and ’622 patents are enforceable, which allegation Aruba denies. Absent a declaration of unenforceability, Wireless Valley will continue wrongfully to assert claims of the ’454 and ’622 patents against Aruba, and thereby cause Aruba irreparable injury and damage.

99. As set forth above, one or more people substantively involved in the prosecution of the application leading to the ’454 and ’622 patents were aware of information material to the patentability of the claims of the ’454 and ’622 patents, but withheld that information from the U.S. Patent and Trademark Office with the intent to deceive, during the prosecution of the ’454 and ’622 patents. In addition, with respect to the ’622 patent, and as set forth above, Aruba is informed and believes, and on that basis alleges, that individuals charged with a duty of candor on behalf of Wireless Valley made false and misleading statements to the U.S. Patent and Trademark Office during the prosecution of the ’622 patent.

100. In light of the above, the ’454 and ’622 patents are not enforceable due to inequitable conduct.

COUNT 7

INFRINGEMENT OF THE ’524 PATENT

101. Aruba incorporates Paragraphs 1 through 68 and 71 through 100 here.

102. Aruba is the sole owner of United States Patent No. 7,295,524 ("the '524 Patent"), entitled "Methods, Apparatuses and Systems Facilitating Management of Airspace in Wireless Computer Network Environments," duly and legally issued by the Patent Office on November 13, 2007 to Gordon Paul Gray, Jason Edward Luther, and Daniel Thomas Augustine. A copy of the '524 Patent is attached hereto as Exhibit A.

103. On information and belief, Motorola, Symbol, and Wireless Valley have been and currently are infringing, contributing to the infringement of, and/or inducing the infringement of the '524 Patent by, among other things, making, using, selling, offering to sell, and/or importing within the territorial boundaries of the United States, products and services—including but not limited to, wireless switches, access points, and other hardware and software for use in connection with wireless networks that operate to perform rogue device detection—that are covered by one or more claims of the '524 Patent.

104. On information and belief, Motorola's, Symbol's, and Wireless Valley's infringement of the '524 Patent has been and is willful, and will continue unless enjoined by this Court. Aruba has suffered, and will continue to suffer, irreparable injury as a result of this willful infringement. Pursuant to 35 U.S.C. § 284, Aruba is entitled to damages for infringement and treble damages. Pursuant to 35 U.S.C. § 283, Aruba is entitled to a permanent injunction against further infringement.

105. This case is exceptional and, therefore, Aruba is entitled to attorneys' fees pursuant to 35 U.S.C. § 285.

COUNT 8

INFRINGEMENT OF THE '113 PATENT

106. Aruba incorporates Paragraphs 1 through 68 and 71 through 105 here.

107. Aruba is the sole owner of United States Patent No. 7,376,113 ("the '113 Patent"), entitled "Mechanism for Securely Extending A Private Network," duly and legally issued by the Patent Office on November 13, 2007 to John Richard Taylor, Pradeep J. Iyer, and Randy Chou. A copy of the '113 Patent is attached hereto as Exhibit B.

108. On information and belief, Motorola, Symbol, and Wireless Valley have been and currently are infringing, contributing to the infringement of, and/or inducing the infringement of the ’113 Patent by, among other things, making, using, selling, offering to sell, and/or importing within the territorial boundaries of the United States, products and services—including but not limited to, wireless switches, access points, and other hardware and software for use in connection with wireless networks that operate to securely extend networks—that are covered by one or more claims of the ’113 Patent.

109. On information and belief, Motorola’s, Symbol’s and Wireless Valley’s infringement of the ’113 Patent has been and is willful, and will continue unless enjoined by this Court. Aruba has suffered, and will continue to suffer, irreparable injury as a result of this willful infringement. Pursuant to 35 U.S.C. § 284, Aruba is entitled to damages for infringement and treble damages. Pursuant to 35 U.S.C. § 283, Aruba is entitled to a permanent injunction against further infringement.

110. This case is exceptional and, therefore, Aruba is entitled to attorneys’ fees pursuant to 35 U.S.C. § 285.

DEMAND FOR A JURY TRIAL

111. Aruba requests a trial by jury on all issues so triable.

PRAYER FOR RELIEF

WHEREFORE, Aruba prays the Court as follows:

A. That the Court enter judgment for Aruba against each of Symbol and Wireless Valley on their Complaint;

B. That each of Symbol and Wireless Valley take nothing by their Complaint;

C. That the Court dismiss each of Symbol’s and Wireless Valley’s claims with prejudice;

D. That the Court declare each and every asserted claim of the ’922, ’923, ’454 and ’622 patents to be (a) not infringed by Aruba, (b) invalid, and (c) unenforceable;

E. That, under 35 U.S.C. § 285, the Court deem this to be an exceptional case and that the Court award Aruba its "reasonable attorney fees" against each of Motorola, Symbol, and Wireless Valley;

F. That the Court award Aruba its costs of suit;

G. That Motorola, Symbol and Wireless Valley be adjudged to have infringed the '524 Patent and/or the '113 Patent;

H. That Motorola, Symbol and Wireless Valley, their agents, employees, representatives, successors and assigns, and those persons in active concert or participation with any of them, and their successors and assigns be permanently enjoined from infringement, inducement of infringement, and contributory infringement of the '524 Patent and/or '113 Patent, including but not limited to making, using, offering for sale, selling and importing into the United States any devices or products that infringe the '524 Patent and/or '113 Patent;

I. That Motorola, Symbol and Wireless Valley be adjudged to have willfully infringed the '524 Patent and/or the '113 Patent, and that continued infringement by Motorola, Symbol and Wireless Valley is willful;

J. That the Court award Aruba damages in an amount adequate to compensate for the infringement by Motorola, Symbol and Wireless Valley of the '524 Patent and/or '113 Patent, but in no event less than a reasonable royalty under 35 U.S.C. § 284;

K. That the Court enter an order trebling any and all damages awarded to Aruba by reason of willful infringement by Motorola, Symbol and Wireless Valley of the '524 Patent and/or '113 Patent under 35 U.S.C. § 284;

L. That the Court enter an order awarding Aruba interest on the damages awarded and its costs under 35 U.S.C. § 284; and

M. That the Court award Aruba such other and additional relief as this Court deems just and proper.

/s/ Frederick L. Cottrell, III______
Frederick L. Cottrell, III (#2555)
Richards, Layton & Finger
One Rodney Square
920 North King Street
P. O. Box 551
Wilmington, DE 19899
Telephone: (302) 651-7700
cottrell@rlf.com

Attorneys for Defendant and Counter-Claimant
ARUBA NETWORKS, INC.

Of Counsel:

MATTHEW D. POWERS
WEIL, GOTSHAL & MANGES LLP
Silicon Valley Office
201 Redwood Shores Parkway
Redwood Shores, CA 94065
Telephone: (650) 802-3000

NICHOLAS GROOMBRIDGE
PAUL E. TORCHIA
ETAI LAHAV
WEIL, GOTSHAL & MANGES LLP
New York Office
767 Fifth Avenue
New York, NY 10153-0119
Telephone: (212) 310-8000

Dated: July 16, 2008

EXHIBIT A

US007295524B1

(12) **United States Patent**
Gray et al.

(10) **Patent No.: US 7,295,524 B1**
(45) **Date of Patent: Nov. 13, 2007**

(54) **METHODS, APPARATUSES AND SYSTEMS FACILITATING MANAGEMENT OF AIRSPACE IN WIRELESS COMPUTER NETWORK ENVIRONMENTS**

(75) Inventors: **Gordon Paul Gray**, Menlo Park, CA (US); **Jason Edward Luther**, San Francisco, CA (US); **Daniel Thomas Augustino**, San Francisco, CA (US)

(73) Assignee: **Airwave Wireless, Inc**, San Mateo, CA (US)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 1005 days.

(21) Appl. No.: **10/368,152**

(22) Filed: **Feb. 18, 2003**

(51) **Int. Cl.**
H04L 12/28 (2006.01)

(52) **U.S. Cl.** **370/254**; 370/338

(58) **Field of Classification Search** .... None
See application file for complete search history.

(56) **References Cited**

U.S. PATENT DOCUMENTS

6,363,421	B2 *	3/2002	Barker et al.	709/223
6,957,067	B1 *	10/2005	Iyer et al.	455/435.1
7,068,999	B2 *	6/2006	Ballai	455/411
2002/0191548	A1 *	12/2002	Ylonen et al.	370/254
2004/0049699	A1 *	3/2004	Griffith et al.	713/201
2004/0203593	A1 *	10/2004	Whelan et al.	455/411

OTHER PUBLICATIONS

J. Case et al., "RFC 1157—A Simple Network Management Protocol (SNMP)", 1990, pp. cover.*

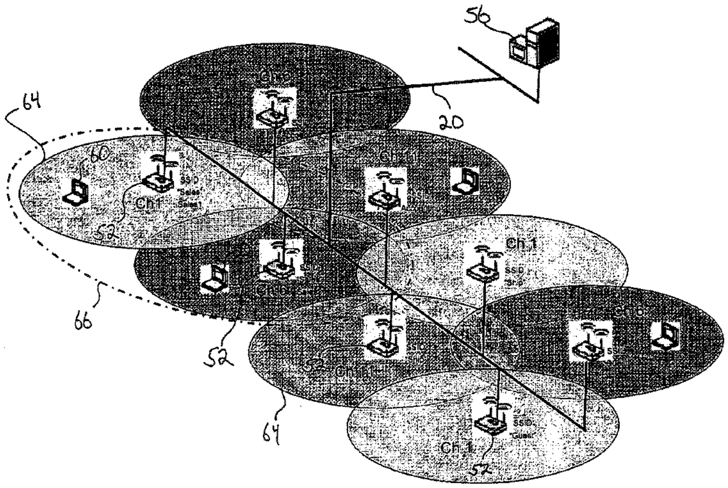
* cited by examiner

Primary Examiner—Chau Nguyen
Assistant Examiner—Jung Park
(74) *Attorney, Agent, or Firm*—Dickstein Shapiro LLP

(57) **ABSTRACT**

Methods, apparatuses and systems facilitating the management of wireless computer network environments and the detection of rogue and other devices that may affect the performance and/or security of the wireless computer network. The present invention enables accurate and cost effective WLAN airspace mapping. In one embodiment, the present invention allows any conforming access point the ability to routinely scan its airspace, collect data on all operating frequencies and report this information back to a management platform. In one embodiment, the management and reporting functionality described herein uses a standards-based vehicle, such as Simple Network Management Protocol (SNMP). In one embodiment, the present invention allows for detection of all wireless traffic within or affecting an enterprise's computer network environment, picking up all active access points (Ad Hoc or Infrastructure) and all wireless clients data regardless of SSID, channel, or security settings. The management platform, according to an embodiment of the present invention, analyzes information received from the access points under management to detect and report the state of the computer network environment. In one embodiment, the present invention facilitates isolation of rogue wireless devices affecting the computer network environment and effective decision-making as to management of the detected device. The present invention also allows network administrators to optimize the configuration of the wireless network environment for performance and security.

14 Claims, 12 Drawing Sheets



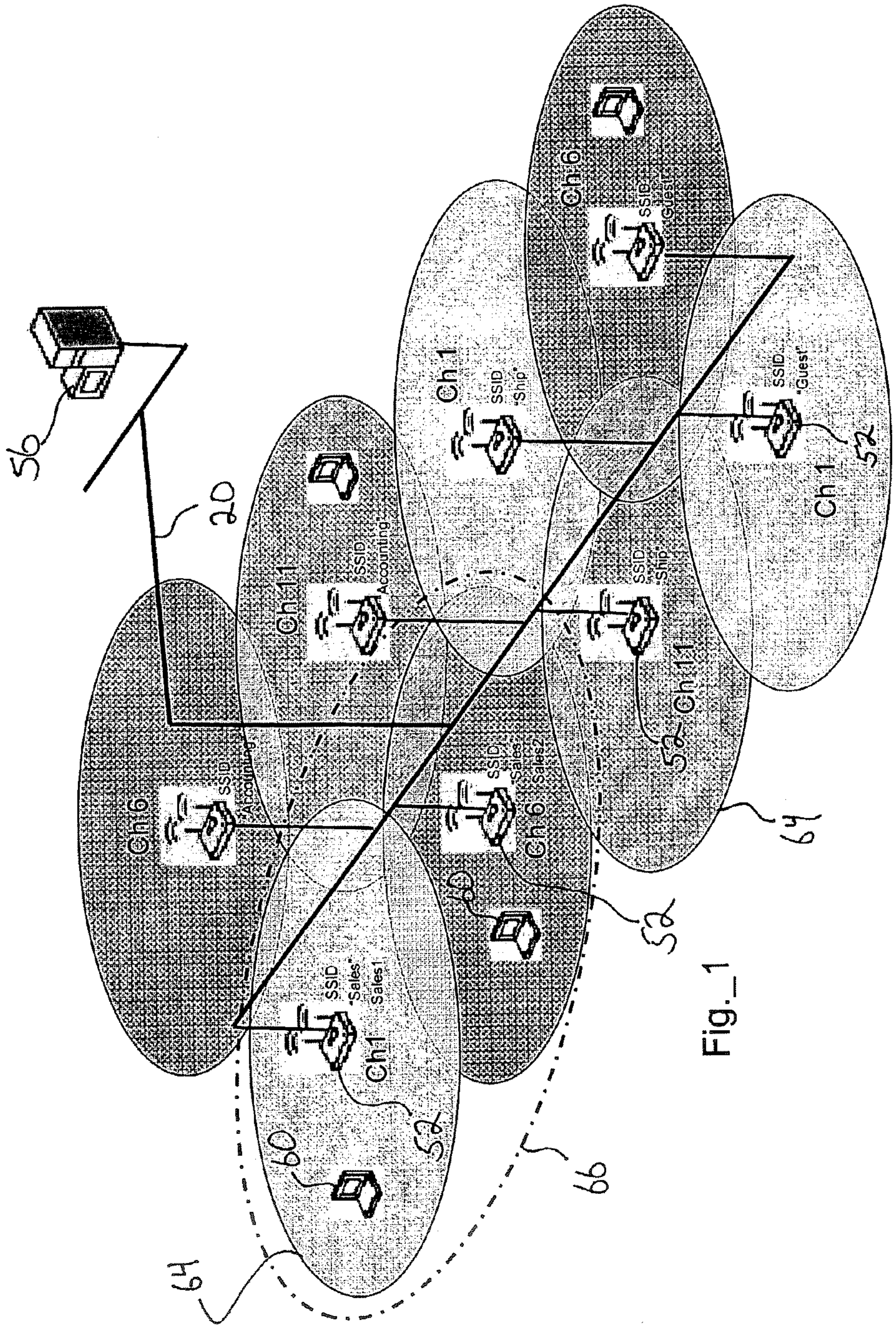
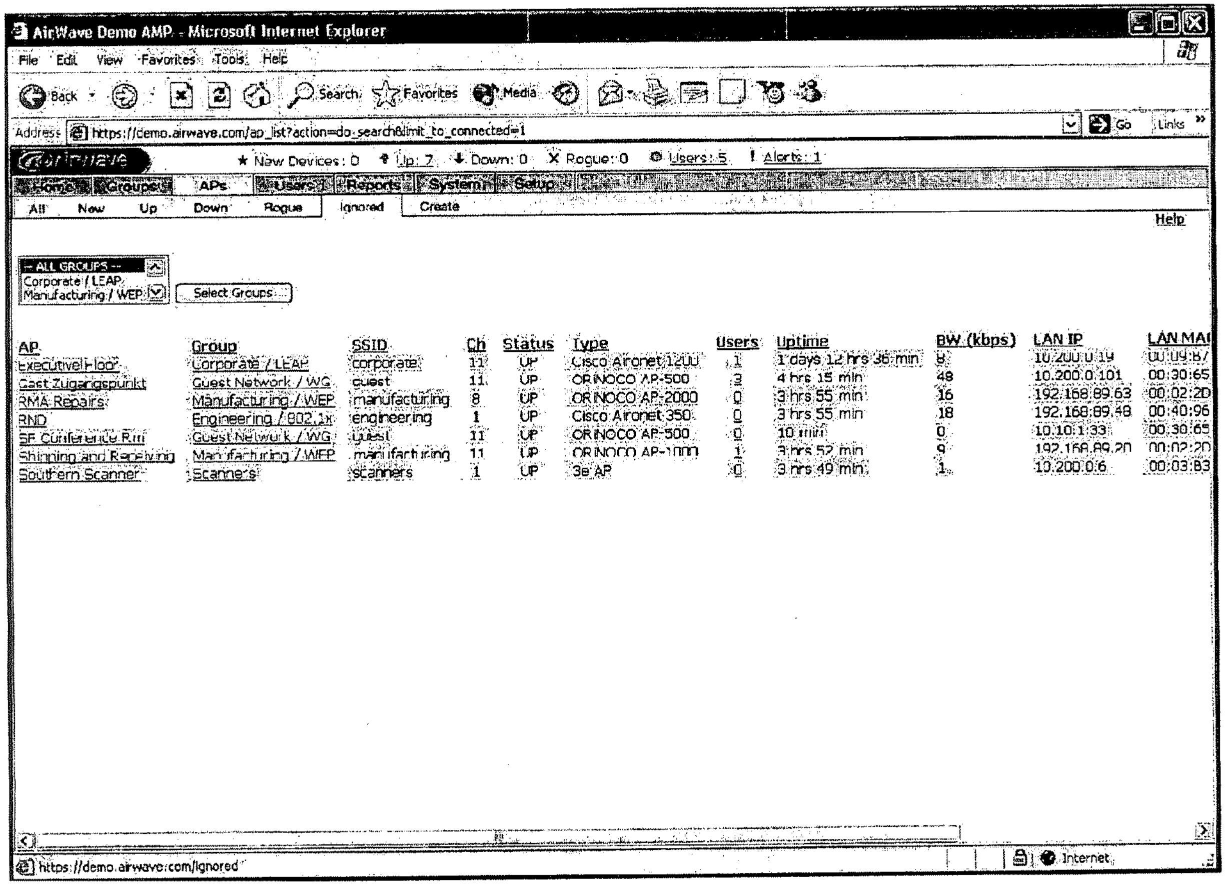
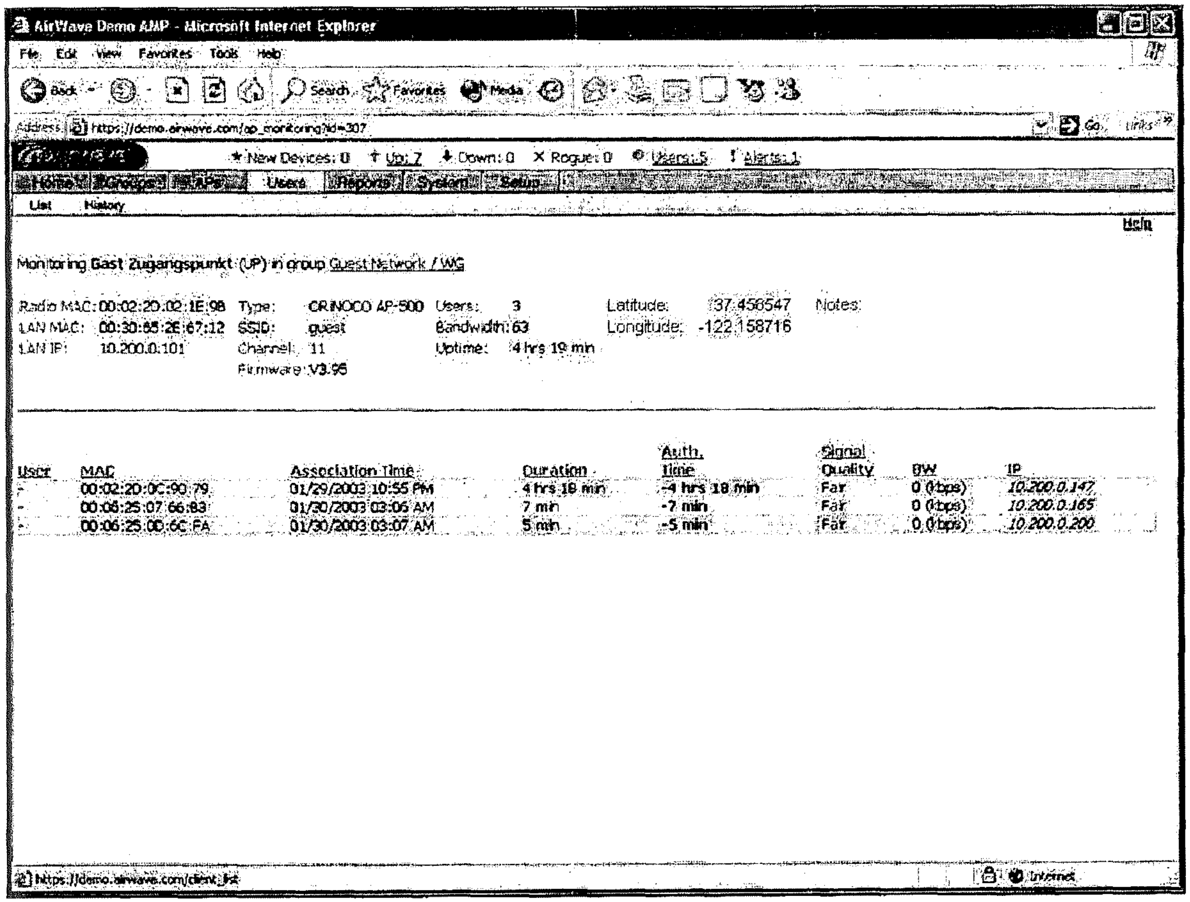

Ch 6
SSID "Guest"
Ch 1
SSID "Ship"
SSID "Guest"
52
Ch 1
Ch 11
SSID "Accounting"
56
20
SSID "Ship"
Ch 11
52
64
Ch 6
SSID "Accounting"
SSID "Sales" "Sales2"
Ch 6
60
52
SSID "Sales" "Sales1"
Ch 1
52
60
66
64

Fig._1


AirWave Demo AMP - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address https://demo.airwave.com/ap_list?action=do_search&limit_to_connected=1
Go Links »
airwave
★ New Devices: 0 ↑ Up: 7 ↓ Down: 0 X Rogue: 0 Users: 5 ! Alerts: 1
Home Groups APs Users Reports System Setup
All New Up Down Rogue Ignored Create
Help
-- ALL GROUPS --
Corporate / LEAP
Manufacturing / WEP
Select Groups...
https://demo.airwave.com/ignored
Internet

AP	Group	SSID	Ch	Status	Type	Users	Uptime	BW (kbps)	LAN IP	LAN MA
Executive Floor	Corporate / LEAP	corporate	11	UP	Cisco Aironet 1200	1	1 days 12 hrs 36 min	8	10.200.0.19	00:09:B7
Gast Zugangspunkt	Guest Network / WG	guest	11	UP	ORINOCO AP-500	3	4 hrs 15 min	48	10.200.0.101	00:30:65
RMA Repairs	Manufacturing / WEP	manufacturing	8	UP	ORINOCO AP-2000	0	3 hrs 55 min	16	192.168.89.63	00:02:2D
RND	Engineering / 802.1x	engineering	1	UP	Cisco Aironet 350	0	3 hrs 55 min	18	192.168.89.48	00:40:96
SF Conference Rm	Guest Network / WG	guest	11	UP	ORINOCO AP-500	0	10 min	0	10.10.1.33	00:30:65
Shipping and Receiving	Manufacturing / WEP	manufacturing	11	UP	ORINOCO AP-1000	1	3 hrs 52 min	9	192.168.89.20	00:02:2D
Southern Scanner	Scanners	scanners	1	UP	3e AP	0	3 hrs 49 min	1	10.200.0.6	00:03:B3

Fig._2

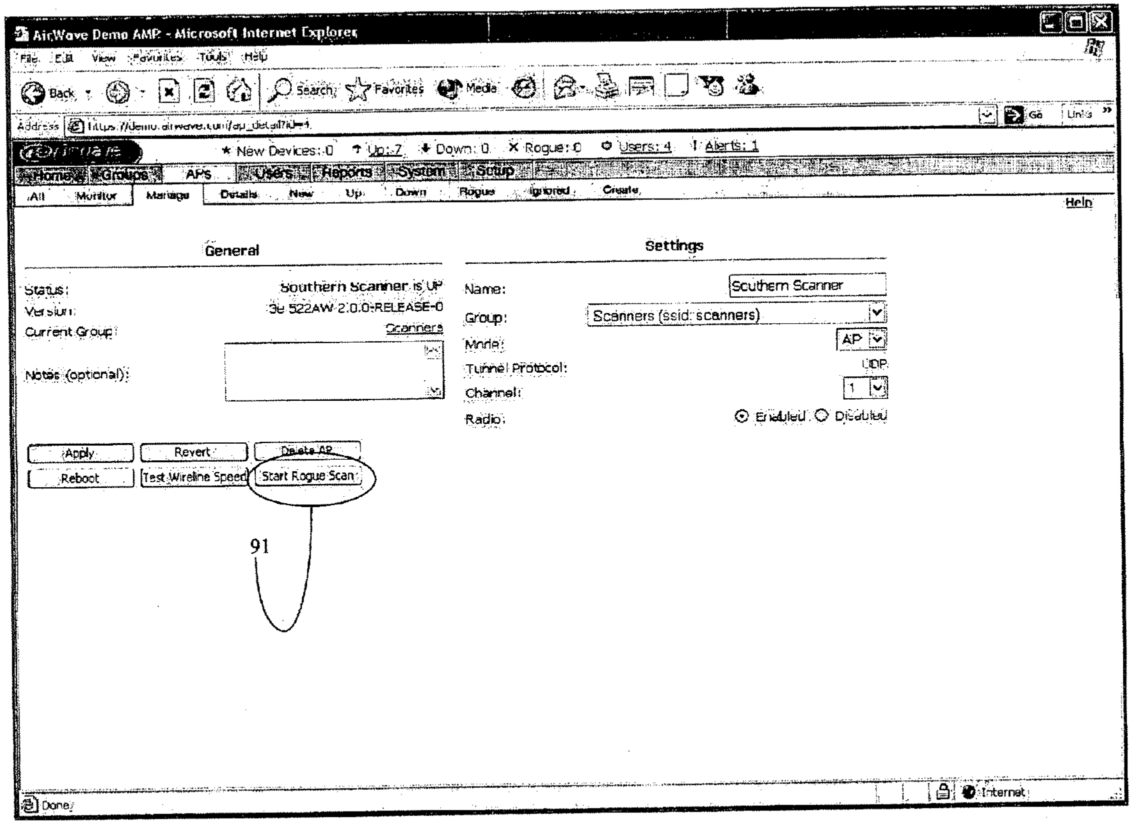

AirWave Demo AMP - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back
Search
Favorites
Media
Address https://demo.airwave.com/ap_monitoring?id=307
Go
Links
New Devices: 0
Up: 7
Down: 0
Rogue: 0
Users: 5
Alerts: 1
Home
Groups
APs
Users
Reports
System
Setup
List
History
Help
https://demo.airwave.com/client_list
Internet

Monitoring Gast Zugangspunkt (UP) in group Guest Network / WG

Radio MAC:	00:02:20:02:1E:98	Type:	ORINOCO AP-500	Users:	3	Latitude:	37.456547	Notes:
LAN MAC:	00:30:65:2E:67:12	SSID:	guest	Bandwidth:	63	Longitude:	-122.158716	
LAN IP:	10.200.0.101	Channel:	11	Uptime:	4 hrs 19 min			
		Firmware:	V3.95					

User	MAC	Association Time	Duration	Auth. Time	Signal Quality	BW	IP
-	00:02:20:0C:90:79	01/29/2003 10:55 PM	4 hrs 18 min	-4 hrs 18 min	Fair	0 (0bps)	10.200.0.147
-	00:06:25:07:66:83	01/30/2003 03:06 AM	7 min	-7 min	Fair	0 (0bps)	10.200.0.165
-	00:06:25:00:6C:FA	01/30/2003 03:07 AM	5 min	-5 min	Fair	0 (0bps)	10.200.0.200

Fig._3



General

Status: Southern Scanner is UP

Version: 3e 522AW 2.0.0-RELEASE-0

Current Group: Scanners

Notes (optional):

Settings

Name: Scuthern Scanner

Group: Scanners (ssid: scanners)

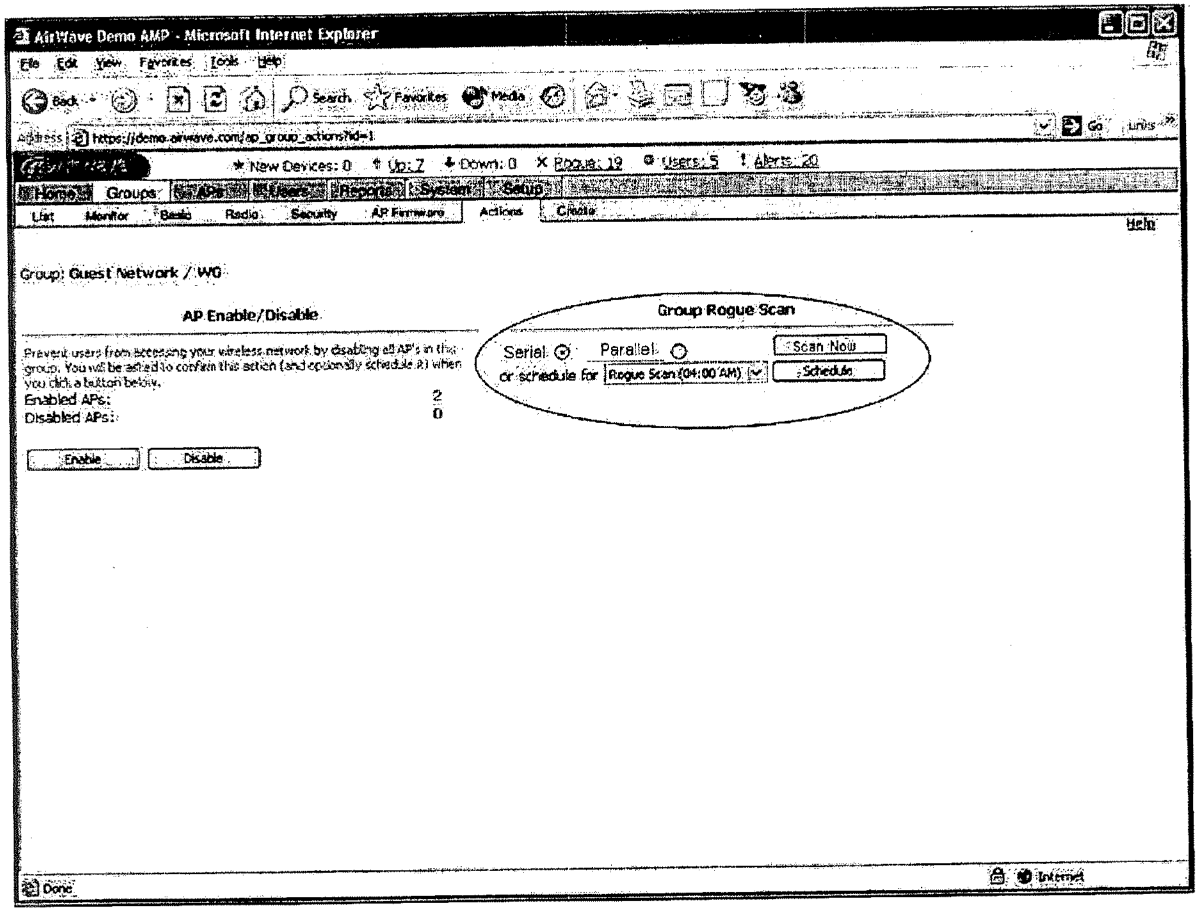
Mode: AP

Tunnel Protocol: UDP

Channel: 1

Radio: ● Enabled ○ Disabled

Fig._4


AirWave Demo AMP - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address https://demo.airwave.com/ap_group_actions?id=1
Go Links
★ New Devices: 0 ↑ Up: 7 ↓ Down: 0 ✕ Rogue: 19 Users: 5 ! Alerts: 20
Home Groups APs Users Reports System Setup
List Monitor Basic Radio Security AP Firmware Actions Create
Help
Enable
Disable
Scan Now
Schedule
Done
Internet

Group: Guest Network / W0

AP Enable/Disable

Prevent users from accessing your wireless network by disabling all AP's in this group. You will be asked to confirm this action (and optionally schedule it) when you click a button below.

Enabled APs: 2
Disabled APs: 0

Group Rogue Scan

Serial: ● Parallel: ○

or schedule for Rogue Scan (04:00 AM)

Fig._5

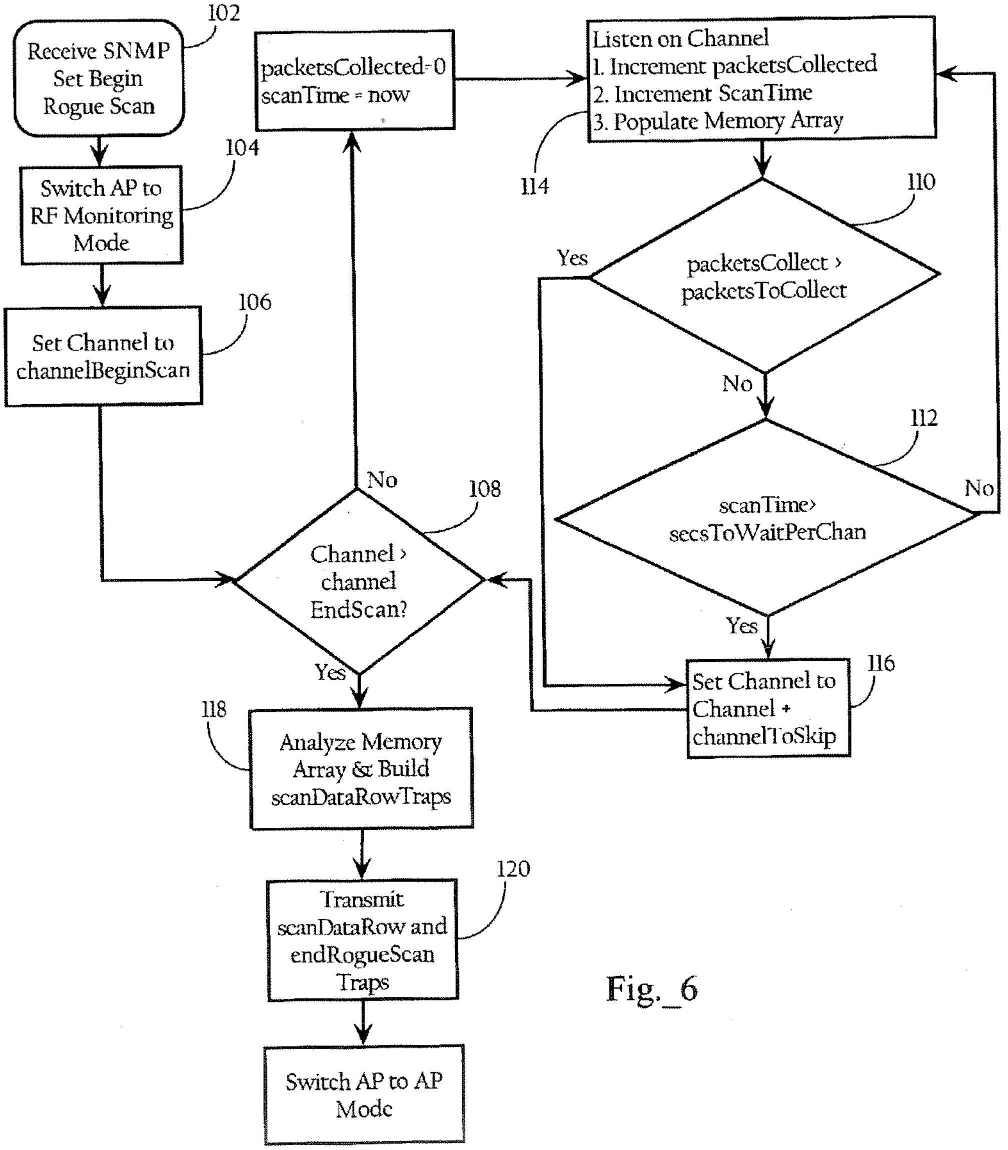
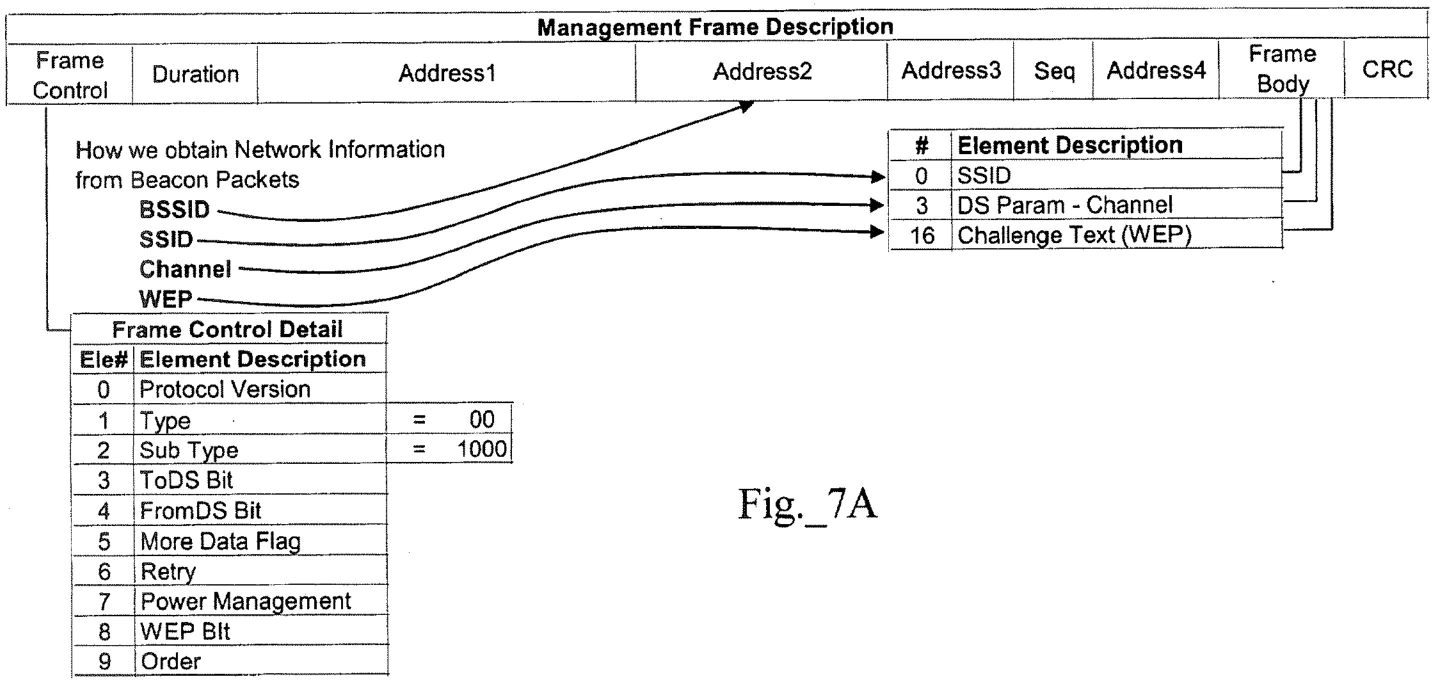

Receive SNMP Set Begin Rogue Scan
102
Switch AP to RF Monitoring Mode
104
Set Channel to channelBeginScan
106
packetsCollected=0
scanTime = now
Listen on Channel
1. Increment packetsCollected
2. Increment ScanTime
3. Populate Memory Array
114
110
Yes
packetsCollect > packetsToCollect
No
112
No
scanTime> secsToWaitPerChan
Yes
No
108
Channel > channel EndScan?
Yes
Set Channel to Channel + channelToSkip
116
118
Analyze Memory Array & Build scanDataRowTraps
120
Transmit scanDataRow and endRogueScan Traps
Switch AP to AP Mode

Fig._6



Management Frame Description								
Frame Control	Duration	Address1	Address2	Address3	Seq	Address4	Frame Body	CRC

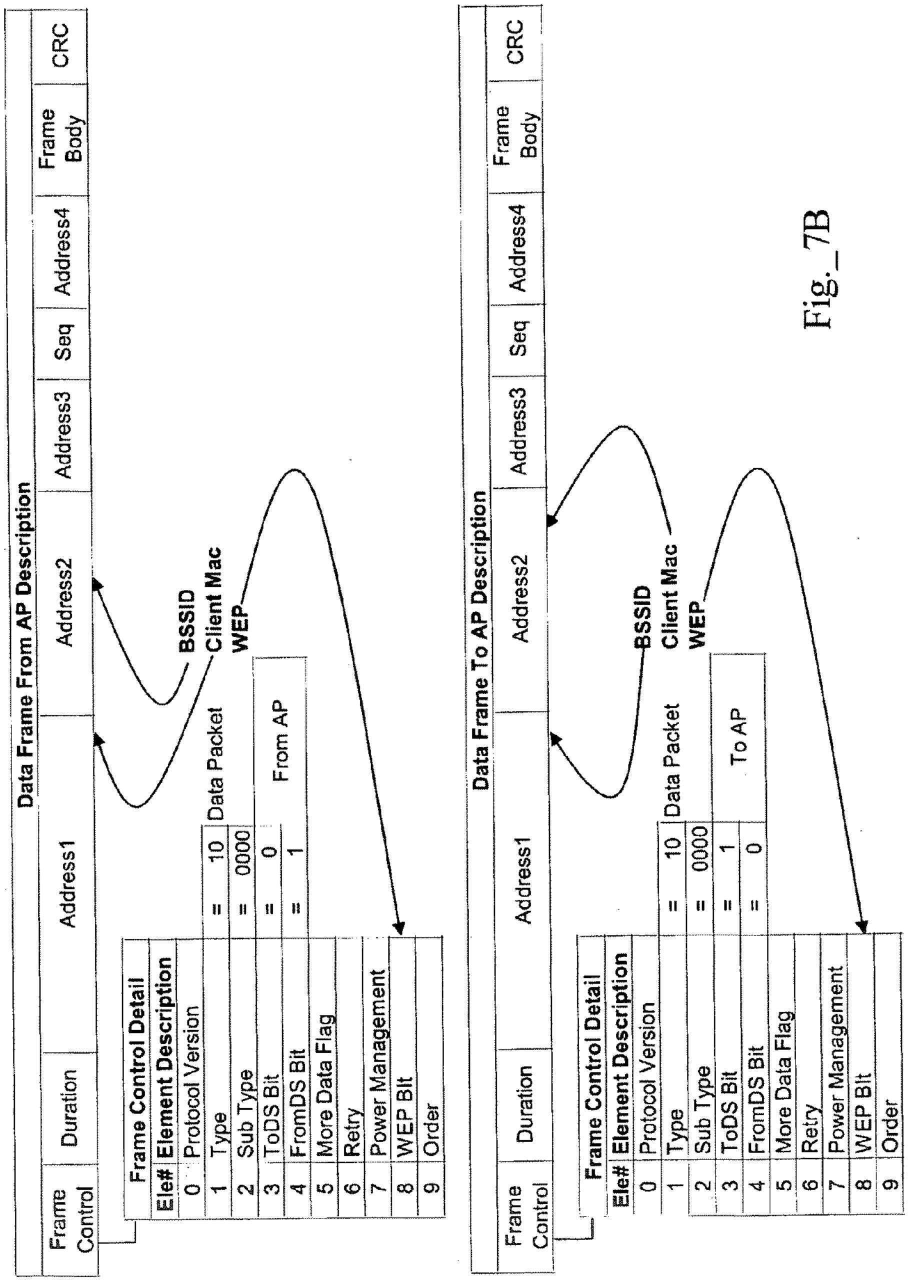
How we obtain Network Information from Beacon Packets

#	Element Description
0	SSID
3	DS Param - Channel
16	Challenge Text (WEP)

Frame Control Detail

Ele#	Element Description		
0	Protocol Version		
1	Type	=	00
2	Sub Type	=	1000
3	ToDS Bit		
4	FromDS Bit		
5	More Data Flag		
6	Retry		
7	Power Management		
8	WEP BIt		
9	Order		

Fig._7A



Data Frame From AP Description

Frame Control	Duration	Address1	Address2	Address3	Seq	Address4	Frame Body	CRC

Frame Control Detail

Ele#	Element Description			
0	Protocol Version			
1	Type	=	10	Data Packet
2	Sub Type	=	0000	
3	ToDS Bit	=	0	From AP
4	FromDS Bit	=	1	
5	More Data Flag			
6	Retry			
7	Power Management			
8	WEP Bit			
9	Order			

Data Frame To AP Description

Frame Control	Duration	Address1	Address2	Address3	Seq	Address4	Frame Body	CRC

Frame Control Detail

Ele#	Element Description			
0	Protocol Version			
1	Type	=	10	Data Packet
2	Sub Type	=	0000	
3	ToDS Bit	=	1	To AP
4	FromDS Bit	=	0	
5	More Data Flag			
6	Retry			
7	Power Management			
8	WEP Bit			
9	Order			

Fig._7B

AP Memory Buffer During Rogue AP Scan

Scanning Channel	Packet Type	BSSID	Client MAC	SSID	WEP	Type	Channel	RSSI
1	Data	00:02:2D:03:4C:B0	00:02:2D:56:5B:FF		No	Client	1	
2	Data	00:02:2D:03:4C:B0	00:02:2D:56:5B:FF		No	Client	2	
3	Beacon	00:02:2D:03:4C:B0		AirPort Network	No	AP	1	30
3	Data	00:02:2D:03:4C:B0	00:02:2D:56:5B:FF		No	Client	3	
4	Beacon	00:02:2D:03:4C:B0		AirPort Network	No	AP	1	26
5	Data	00:03:2F:00:12:AE	00:06:25:0D:6E:16		No	Client	5	
6	Data	00:03:2F:00:12:AE	00:06:25:0D:6E:16		No	Client	6	
7	Data	00:03:2F:00:12:AE	00:06:25:0D:6E:16		No	Client	7	
8	No Data							
9	Data	00:02:2D:0D:4D:7C	00:06:25:0D:AA:11		No	Client	9	
10	Data	00:02:2D:0D:4D:7C	00:06:25:0D:AA:11		No	Client	10	
11	Data	00:02:2D:0D:4D:7C	00:06:25:0D:AA:11		No	Client	11	

Post Analysis Data Sent via SNMP Traps to AMP from Scanning AP

awAPScanID	awAPReturnBSSID	awAPReturnSSID	awAPReturnChannel	awAPReturnWepOn	awAPReturnType	awAPReturnRSSI	awAPReturnCLMAC
00:03:2F:00:79:FE	00:02:2D:03:4C:B0	AirPort Network	1	1	1	28	
00:03:2F:00:79:FE	00:02:2D:03:4C:B0	AirPort Network	1	1	2		00:02:2D:56:5B:FF
00:03:2F:00:79:FE	00:03:2F:00:12:AE		6	1	2		00:06:25:0D:6E:16
00:03:2F:00:79:FE	00:02:2D:0D:4D:7C		11	1	2		00:06:25:0D:AA:11

Fig._8

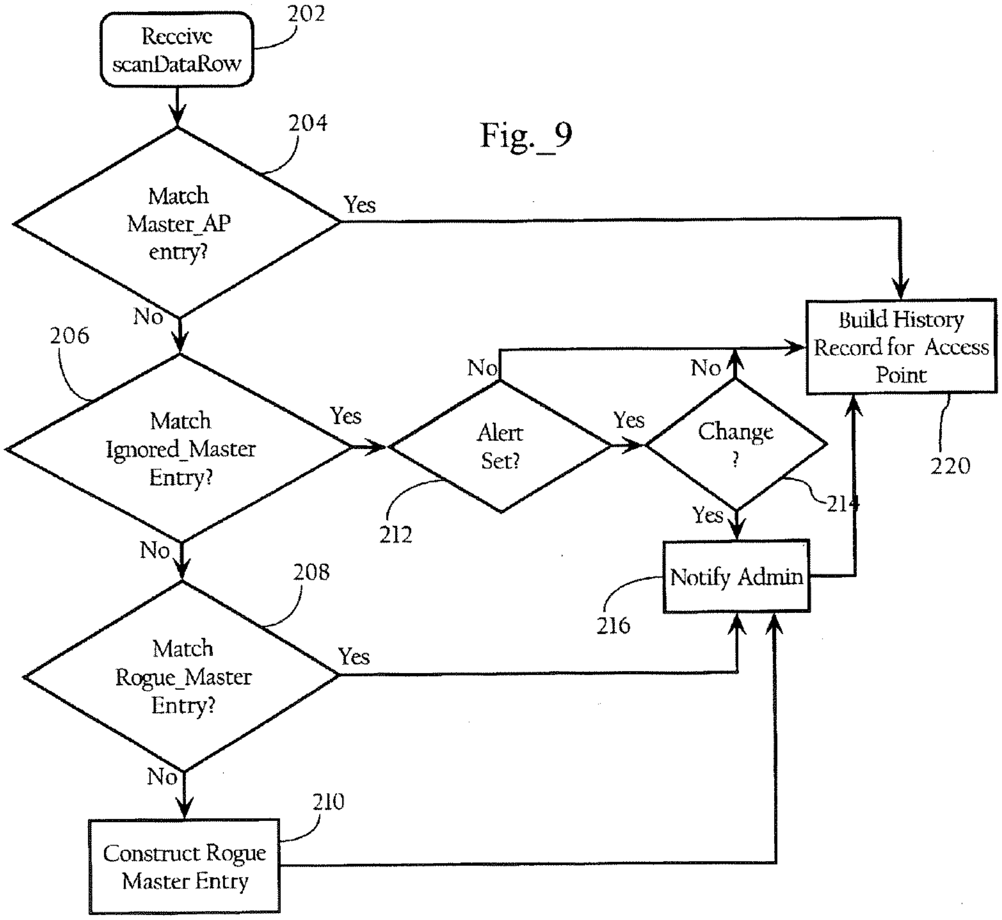
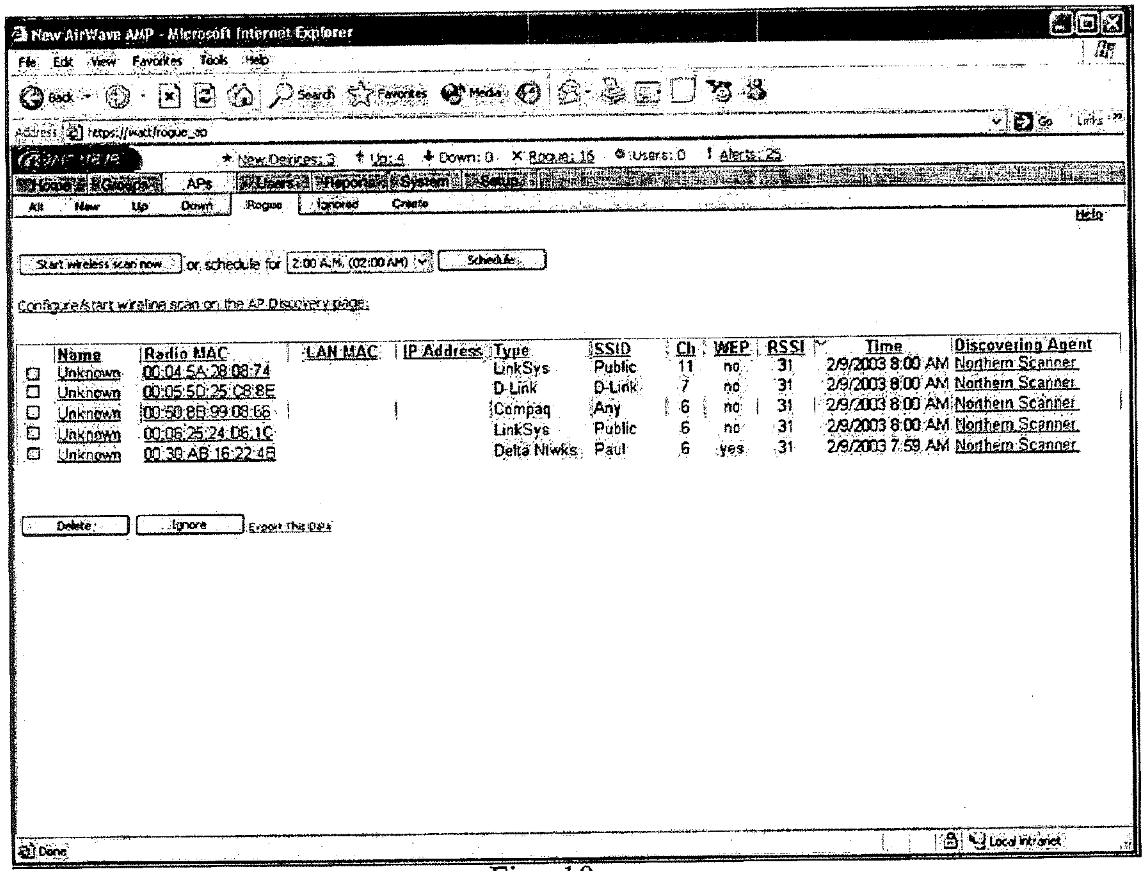

Reccive scanDataRow
202
Match Master_AP entry?
204
Yes
No
206
Match Ignored_Master Entry?
Yes
No
Alert Set?
212
No
Yes
Change ?
214
No
Yes
Build History Record for Access Point
220
Notify Admin
216
208
Match Rogue_Master Entry?
Yes
No
210
Construct Rogue Master Entry

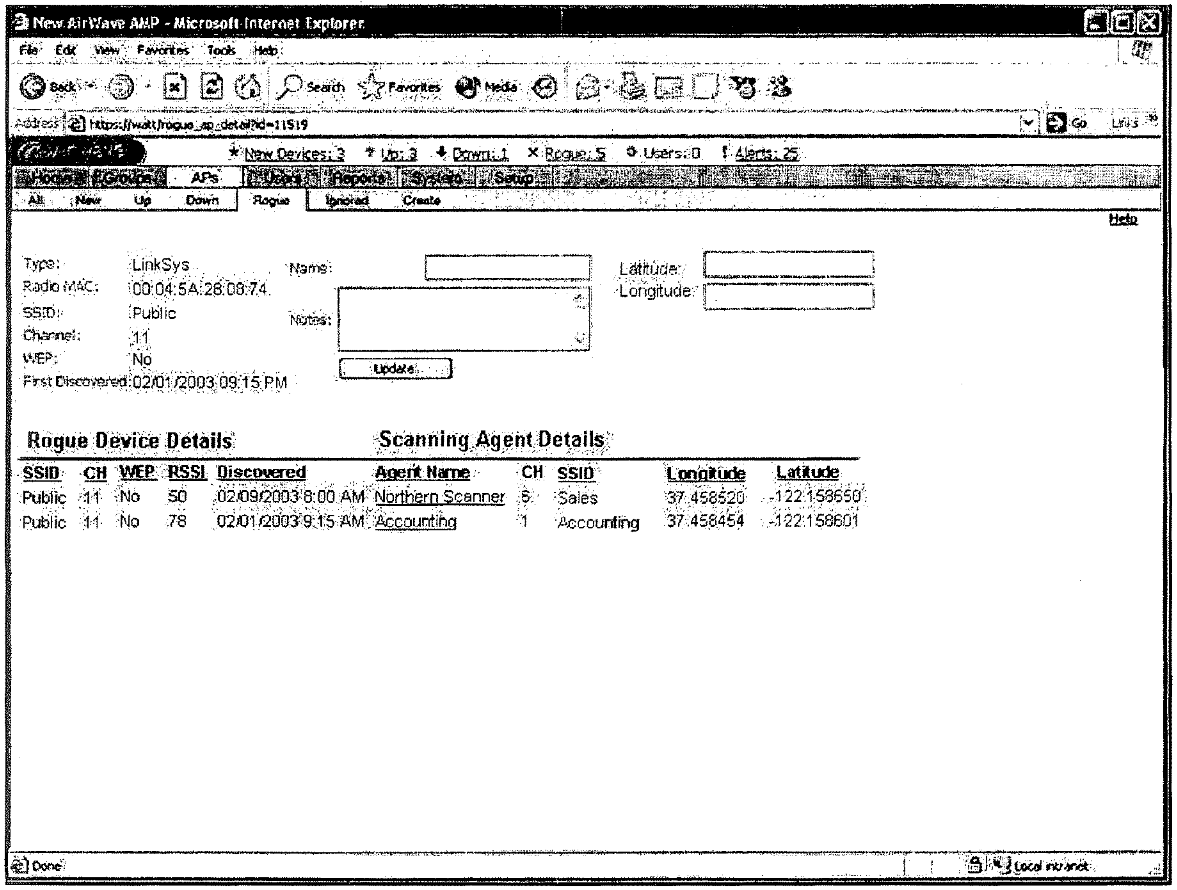
Fig._9


New AirWave AMP - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address https://watt/rogue_ap
Go Links
★ New Devices: 3 ↑ Up: 4 ↓ Down: 0 ✕ Rogue: 16 ⚙ Users: 0 ! Alerts: 25
Home Groups APs Users Reports System Setup
All New Up Down Rogue Ignored Create
Help
Start wireless scan now
Schedule
Configure/start wireline scan on the AP Discovery page.
Delete
Ignore
Export This Data
Done
Local intranet

or schedule for 2:00 A.M. (02:00 AM)

	Name	Radio MAC	LAN MAC	IP Address	Type	SSID	Ch	WEP	RSSI	Time	Discovering Agent
□	Unknown	00:04:5A:28:08:74			LinkSys	Public	11	no	31	2/9/2003 8:00 AM	Northern Scanner
□	Unknown	00:05:5D:25:C8:8E			D-Link	D-Link	7	no	31	2/9/2003 8:00 AM	Northern Scanner
□	Unknown	00:50:8B:99:08:66			Compaq	Any	6	no	31	2/9/2003 8:00 AM	Northern Scanner
□	Unknown	00:06:25:24:D6:1C			LinkSys	Public	6	no	31	2/9/2003 8:00 AM	Northern Scanner
□	Unknown	00:30:AB:16:22:4B			Delta Ntwks	Paul	6	yes	31	2/9/2003 7:59 AM	Northern Scanner

Fig._10


New AirWave AMP - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address https://watt/rogue_ap_detail?id=11519
Go Links
New Devices: 3 Up: 3 Down: 1 Rogue: 5 Users: 0 Alerts: 25
Home Groups APs Users Reports System Setup
All New Up Down Rogue Ignored Create
Help
Update
Done
Local intranet

Type: LinkSys
Radio MAC: 00:04:5A:28:08:74
SSID: Public
Channel: 11
WEP: No
First Discovered: 02/01/2003 09:15 PM

Name:
Notes:

Latitude:
Longitude:

Rogue Device Details

Scanning Agent Details

SSID	CH	WEP	RSSI	Discovered	Agent Name	CH	SSID	Longitude	Latitude
Public	11	No	50	02/09/2003 8:00 AM	Northern Scanner	6	Sales	37.458520	-122.158650
Public	11	No	78	02/01/2003 9:15 AM	Accounting	1	Accounting	37.458454	-122.158601

Fig._11

METHODS, APPARATUSES AND SYSTEMS FACILITATING MANAGEMENT OF AIRSPACE IN WIRELESS COMPUTER NETWORK ENVIRONMENTS

COPYRIGHT NOTICE

FIELD OF THE INVENTION

The present invention relates to wireless computer networks and, more particularly, to methods, apparatuses and systems facilitating monitoring and management tasks associated with wireless computer networks including wireless access points and wireless clients.

BACKGROUND OF THE INVENTION

In 1997, the Institute of Electrical and Electronics Engineers (IEEE) approved 802.11 the first internationally sanctioned wireless LAN (WLAN) standard. The IEEE 802.11 standard establishes specifications for the parameters of both the physical (PHY) and media access control (MAC) layers of the network. The Institute of Electrical and Electronics Engineers (IEEE) ratified the original 802.11 standards as the standard for WLANs. The initial standard provided 1 Mbps and 2 Mbps transmission rates. This rate of transmission was not sufficient for most general business applications and consequently the rate of adoption was slow.

Recognizing the need for faster transmission speeds, the IEEE ratified the 802.11b standard to allow for transmission speeds of up to 11 Mbps. This new standard now aligns wireless connectivity on comparable levels to wired Ethernet LANs. The range for WLANs depends largely on the medium by which the radio waves are transmitted and the strength of the transmitting antenna. Open air ranges are much longer than if several walls come between the antennas. Depending on the type of radio antenna (omni-directional, bi-directional, etc.) and transmitter strength, optimal distances can vary from 200 feet to 10 miles. Fallback speeds of 5.5, 2, and 1 Mbps occur when optimal distances for transmission are exceeded.

The first 802.11 standard proposed three implementations for the Physical Layer (PHY): Infrared (IR) Pulses Position Modulation, RF Signaling using Frequency Hopping Spread Spectrum (FHSS), and Direct Sequence Spread Spectrum (DSSS). Two working groups were established to explore alternate implementations of the 802.11 standard. Working Group A explored the 5.0 GHz band, while Working Group B focused on the 2.4 GHz band. Wireless communications take place within an area known as the Basic Service Area defined by the propagation characteristics of the wireless medium. A wireless node communicates via a Basic Service Set (BSS) within a basic service area. There are two basic service sets independent and Infrastructure. The independent service set allows wireless stations to operate in a peer-to-peer or Ad Hoc mode. In the ad-hoc network, computers are brought together to form a network "on the fly." There is no structure to the network; there are no fixed points; and usually every node is able to communicate with every other node. Although it seems that order would be difficult to maintain in this type of network, algorithms such as the spokesman election algorithm (SEA) have been designed to select one wireless node as the base station (master) of the network with the others being slaves. The infrastructure service set is the more common approach involving access points (APs) that allow for and control access to the wireless network. An access point usually contains a transceiver, a wired network interface (e.g., 802.3) and software for data processing. If service areas of access points overlap, hand-offs of wireless clients between access points can occur.

Wireless local area networks (WLANs), need their air space to be consistently mapped in order to maintain optimum speed and reliability. In an Ethernet LAN (IEEE 802.3), the Carrier Sense Multiple Access with Collision Detection (CSMA/CD) protocol establishes how simultaneous transmissions (packet collisions) are handled. In a WLAN, collision detection in this manner is not possible due to what is known as the "near/far" problem: to detect a collision, a station must be able to transmit and listen at the same time. To account for this difference, the 802.11 protocol uses a slightly different protocol known as Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) or the Distributed Coordination Function (DCF). CSMA/CA attempts to avoid packet collisions by using explicit packet acknowledgement (ACK), which means that an ACK packet is sent by the receiving station to confirm that a packet arrived intact. CSMA/CA works by having the transmitting wireless station sense the air. If there is no activity detected, the transmitting wireless station will wait an additional random period of time. If there still is no activity, the wireless station transmits the data. If the packet is received intact, the receiving station will send and ACK frame that, once received by the original sender, completes the transmission. If the ACK command is not received in a specified random period of time, the data packet will be resent, assuming that the original packet experienced a collision. CSMA/CA will also handle other interference and radio-wave related problems effectively, but creates considerable overhead.

Given the collision avoidance mechanisms employed in 802.11-compliant wireless networks, management and monitoring of the wireless network airspace (for example, to ensure that wireless access points do not interfere with one another) is critical to the performance of the wireless network environment. The administrative or management functionality associated with WLAN networks, however, generally lacks a reliable and accurate means of collecting, storing, and relating airspace data. Hand-held scanners, AP startup scans, or full-time scanning devices are the current methods of obtaining WLAN air space data. However, these methods are inherently flawed or not cost effective. Accordingly, most WLANs do not perform at optimum speed due to overlapping channel interference and rogue access points (i.e., access points installed without authorization and/or knowledge of a network administrator).

In light of the foregoing, a need in the art exists for methods, apparatuses and systems that allow for efficient mapping of the air space associated with wireless networks. A need further exists for methods, apparatuses and systems that facilitate detection of rogue or unauthorized wireless access points. Embodiments of the present invention substantially fulfill these needs.

SUMMARY OF THE INVENTION

The present invention provides methods, apparatuses and systems facilitating the management of wireless computer network environments and the detection of rogue and other devices that may affect the performance and/or security of the wireless computer network. The present invention enables accurate and cost effective WLAN air space mapping. In one embodiment, the present invention allows any conforming access point the ability to routinely scan its airspace, collect data on all operating frequencies and report this information back to a management platform. In one embodiment, the management and reporting functionality described herein uses a standards-based vehicle, such as Simple Network Management Protocol (SNMP). In one embodiment, the present invention allows for detection of all wireless traffic within or affecting an enterprise's computer network environment, picking up all active access points (Ad Hoc or Infrastructure) and all wireless clients data regardless of SSID, channel, or security settings. The management platform, according to an embodiment of the present invention, analyzes information received from the access points under management to detect and report the state of the computer network environment. In one embodiment, the present invention facilitates isolation of rogue wireless devices affecting the computer network environment and effective decision-making as to management of the detected device. The present invention also allows network administrators to optimize the configuration of the wireless network environment for performance and security.

DESCRIPTION OF THE DRAWINGS

FIG. **1** is a functional block diagram illustrating a wireless computer network environment according to an embodiment of the present invention.

FIG. **2** shows a user interface providing a detailed list of managed wireless access points.

FIG. **3** sets forth a user interface providing detailed information associated with a given wireless access point.

FIG. **4** provides a user interface that allows a user to initiate a scan at a given access point for rogue devices operating within its airspace.

FIG. **5** illustrates a user interface allowing a network administrator to initiate a scan for rogue access points for a group of wireless access points.

FIG. **6** is a flow chart diagram showing a method, according to one embodiment, for scanning at an access point for rogue devices.

FIG. 7A illustrates the layout of management frames or packets in 802.11 networks and the mapping of information in the frames.

FIG. 7B provides the layout of data frames or packets in 802.11 networks.

FIG. **8** illustrates a memory buffer constructed during a scan for rogue devices and a table illustrating the elements of SNMP traps summarizing the data in the memory buffer.

FIG. **9** is a flow chart diagram illustrating a method, according to an embodiment of the present invention, directed to the processing of SNMP traps transmitted by scanning access points.

FIG. **10** provides a user interface showing a list of detected rogue access points.

FIG. **11** illustrates a user interface showing a detail view of a given rogue access point detected during a scan.

DESCRIPTION OF PREFERRED EMBODIMENT(S)

I. Computer Network Environment

FIG. **1** illustrates a computer network environment including an embodiment of the present invention. As FIG. **1** illustrates, the present invention, in one embodiment, operates in a computer network environment including a local area network (LAN) **20** interconnecting a plurality of hosts or other end systems, such as servers, network computers, etc., airspace management platform **56**, and at least one wireless access point **52**. Other computer network environments are possible. For example, while FIG. **1** illustrates that airspace management platform **56** and the at least one wireless access point **52** are connected via a LAN **20**, embodiments of the present invention can be deployed across a wide area network, such as the Internet, to allow a network administrator to remotely manage one to a plurality of network access points **52** from distant locations.

Wireless access points **52** can act as a hub to route data between wireless client devices **60** within its coverage area, and/or bridge network traffic between a computer network **20** and one or more wireless client devices **60**. A Basis Service Set (BSS) **64** refers to the wireless network implemented by a given wireless access point **52** that manages and bridges wireless communications for all wireless client devices **60** within its operating range (Basic Service Area (BSA) and operating on the same frequency channel (see FIG. **1**). In 802.11-compliant wireless networks, a Service Set Identifier (SSID), a unique, 32-character identifier attached to the header of data packets transmitted over a WLAN, acts as a form of password or token when wireless client devices **60** attempt to connect to a Basic Service Set. The SSID differentiates one WLAN from another in that all wireless client devices **60** attempting to connect to a specific WLAN must use the same SSID. An Extended Service Set (ESS) **66** refers to two or more Basic Service Sets, having the same SSID, that are interconnected by a Distribution System (DS) (such as an Ethernet LAN **20**), which provides a set of services enabling the transport of data between BSSs.

Wireless access point **52** is operative to dynamically recognize new users/wireless client devices **60** and wirelessly communicate with one to a plurality of wireless client devices **60**. Wireless access point **52** includes a radio frequency transmitter/receiver unit or an infrared transmitter receiver unit, or both. However, any suitable means of wireless communication can be used. Wireless access point **52** can operate in connection with any wireless communications protocol, including 802.11a and 802.11b, as well as Bluetooth. Wireless access point **52** is further operative to allow access to resources operably connected to computer network **20**. In one embodiment, wireless access point **52** is operative to convert all wireless traffic to Ethernet (or other LAN or network protocol) and route it to appropriate systems connected to computer network **20**. Of course, the specific or optimal network protocols used in connection with the present invention may vary with the protocols implemented on LAN **20**. In one embodiment, wireless access point **52** routes all wireless traffic from client devices **60** to a single location in the computer network embodiment (in one embodiment, a secure access server that authenticates users at client devices and controls access to resources connected to computer network **20**). Co-pending and commonly owned U.S. application Ser. No. 10/271,106 filed Oct. 15, 2002 and entitled "Secure Wireless Network Access

Points," (incorporated by reference herein), discloses methods and systems directed to securing wireless network access points. In one embodiment, wireless access point **52** includes tunneling functionality establishing and maintaining a virtual communications tunnel between access point **52** and the secure access server as disclosed in U.S. application Ser. No. 10/271,106, above. However, as one skilled in the art will recognize, the present invention can be applied in connection with a variety of secure and non-secure wireless network access point configurations. In one embodiment, at least one wireless network access point **52** includes scanning agent functionality operative to monitor its surrounding airspace for wireless traffic relative to at least one frequency channel, gather data characterizing detected wireless traffic, and transmit the data to airspace management platform **56** for processing and presentation to a network administrator. In WLAN environments employing 802.11 protocols, the wireless access point(s) **52** are equipped with 802.11-compliant WLAN network interface cards which support Radio Frequency (RF) monitoring mode, as well as the proper device drivers. In one embodiment, the wireless access point **52** includes an SNMP Management Information Base (MIB) for standards-based delivery of the scan data from the access point to the airspace management platform. In one embodiment, the scanning agent is a software daemon that is invoked when an SNMP SET request is received; the scanning agent operates to scan its airspace and transmit SNMP traps characterizing the devices detected within its coverage area and then allows the wireless access point **52** to resume normal operation.

As discussed in more detail below, airspace management platform **56** facilitates management and overview of the wireless access point(s) **52** operably connected to computer network **20** and, in connection with one or more suitable wireless access point(s) **52**, is operative to monitor the wireless network airspace associated with an administrative domain for wireless client devices and/or network access points, including known/authorized and/or rogue devices and access points. As discussed in more detail below, airspace management platform **56**, in one embodiment, allows network administrators to schedule wireless access point(s) **52** to perform regular or intermittent scans, as well as start scans on-demand. Airspace management platform **56** is further operative to receive data from the network access point(s) **52**, interpret the received data, and present it in a variety of interfaces to a network administrator to allow for intelligent, well-informed decision-making as to the computer network domain. In one embodiment, airspace management platform **56** is a Web-based application executed on a server or other computing device operably connected to computer network **20**, and accessible via a client computer including suitable browsing software, such as Microsoft® Internet Explorer®, or Netscape® Navigator browsers. In another embodiment, airspace management platform **56** may reside on a desktop computer associated with a network administrator.

II. Operation

A. Registration and Management of Access Points

Using the airspace management platform **56**, a network administrator registers at least one wireless access point **52** by entering or discovering information unique to the access point, such as BSSID or Wireless MAC address, LAN MAC address, and LAN IP address. As discussed below, BSSID or Wireless MAC address, LAN MAC address, and IP address

are used as indexes in tables or other data structures that store information about each access point. Wireless access point(s) **52** that are registered with the airspace management platform **56** can then be used to scan for rogue access points and client devices, as discussed below. After registration, access points are authorized or brought under management of airspace management platform **56**. The airspace management platform **56** can monitor the registered wireless access point(s) over computer network **20** via Simple Network Management Protocol (SNMP) read community string, and configure the wireless access point(s) **52** via SNMP read-write community string.

In one embodiment, airspace management platform **56** discovers the functionality and other parameters associated with registered wireless access points and populates a database (such as the tables, below) that includes information on each registered wireless access point **52**. Airspace management platform **56**, in one embodiment, supports a variety of Layer 2 discovery protocols such as CDP (Cisco Discovery Protocol), CDP (Cabletron Discovery Protocol, OSUNMS, and WNMS. Layer 2 discovery methods are suitable when airspace management platform **56** is on the same physical network as the access points **52**. Higher layer discovery methods, such as SNMP and HTTP subnet scanning, are valuable for discovering wireless access points **52** on networks in which airspace management platform **56** is not physically located.

A.1. Access Point Master Table

As discussed above, airspace management platform **56** maintains a database storing information relating to the wireless access point(s) within the airspace associated with the computer network domain. In one embodiment, the database is a relational database comprising a plurality of tables, including a Master_AP table, an AP_Capabilities table, as well as other tables set forth below. In one embodiment, airspace management platform **56** creates a record in an AP_Master table including information gathered during the registration and discovery processes. The AP_Master table, in one embodiment, includes the following fields: 1) AP_Name (a user definable field of 32 characters), 2) Wireless Interface MAC address (Media Access Control, a 48-bit address generally displayed as 12 hexadecimal digits), 3) LAN Interface MAC Address, 4) LAN IP, 5) Service Set Identifier, 6) Type (i.e., Manufacturer and Product Name), 7) Firmware Version, 8) Channel, 9) Uptime, 10) Positional Parameters (e.g., Latitude and Longitude), and 11) a RogueScanFlag (indicating whether the wireless access point supports rogue access point scanning). Other fields can include: 12) Group_Name (a user definable field indicating a grouping of access points for administrative purposes, see below), 13) status [up/down], 14) number of users, and 15) bandwidth.

The AP_Master table has several indexes which are employed in rogue access point detection. In one embodiment, the primary keys for the AP_Master table are: AP_Name, LAN Interface MAC Address (LAN_MAC), and Wireless Interface MAC Address (WLAN_MAC). Another field of importance to rogue access point detection in the AP_Master table is the RogueScanFlag. This flag is a Yes/No data type, where "Yes" indicates that the access point supports rogue AP scanning, and "No" indicates that the access point does not support rogue AP scanning. As discussed above, the database maintained by airspace management platform **56** contains an AP_Capabilities table relating AP manufacturer, model, and ability to support rogue scanning. When access points are registered and inserted into the AP_Master table the AP_Capabilities table is queried by manufacturer and model name to correctly set the RogueScanFlag in the AP_Master table.

As FIG. **2** illustrates, airspace management platform **56** provides an overview of the wireless access points, displaying, in one embodiment, a subset of the values or fields of the AP_Master table to the network administrator. As FIG. **3** shows, airspace management platform **56** also allows the user to click on a particular access point in the interface depicted in FIG. **2** to see a detailed view of a desired wireless access point, such as the users currently associated with a wireless access point **52**.

A.2. Administrative Groups

Once registered, wireless access point(s) **52** are ready for inclusion in scans for rogue access points. As discussed above, airspace management platform **56** allows a network administrator to define two or more managed wireless access point(s) into groups for administrative purposes, such as applying configuration changes and the scheduling of rogue access point scans. Airspace management platform **56** allows a network administrator to initiate a scan at the access point level (see FIG. **4**, button **91**), or at the group level (see FIG. **5**). In one embodiment, a "group" encompasses access points sharing similar security and radio characteristics. For example, in the WLAN set forth in FIG. **1**, wireless access points named "Sales1" and "Sales2" are associated with a group defined by a network administrator. These wireless access points share the same SSID and security settings geared for the Sales department or "Sales Group" as defined in airspace management platform **56**. Accordingly, in this example, the employees or other users associated with the sales department would configure their wireless client devices (WLAN network interface cards) to associate with access points having an SSID set to "Sales." In another embodiment, a group is arbitrarily defined by an administrator according to any desired criteria, such as location, department, etc. Groups can be used to simplify administration of a wireless LAN functionality, because configuration changes for a group can be entered once and automatically applied to all wireless access points associated with the group. In addition, groups provide a very efficient way of viewing or monitoring the wireless network. Executing a rogue AP scan by group enables a WLAN administrator to trigger scanning on all wireless access points in the group that have scanning capability with minimal effort.

A.3. Scheduling of AP Scans

As FIG. **5** illustrates, airspace management platform **56** permits the flexibility to scan immediately (on-demand) or schedule a rogue AP scan for a later time. Scheduling is a desirable feature as Rogue AP scans are obtrusive to the WLAN environment. Specifically, when a wireless access point **52** is configured to scan in RF promiscuous mode, it only listens or monitors for wireless traffic, because, given the collision avoidance mechanisms associated with the 802.11 protocols, transmitting data may prevent any incoming traffic it was trying to collect. As one skilled in the art will recognize, other wireless networking protocols may allow wireless access points to simultaneously operate in RF promiscuous mode and access point mode. Accordingly, during a scan, wireless client devices **60** are disconnected from the scanning wireless access point **52** and, therefore, have no connectivity to LAN **20**. Scheduling Rogue AP scans at night or on the weekend reduces the opportunities that wireless client devices **60** experience a loss of network connectivity. As FIG. **5** illustrates, airspace management platform **56** also supports both serial and parallel methods of executing the scan within a group as to both scheduled scans and on-demand scans. Serial scanning enables a well designed wireless LAN to maintain wireless client connectivity, because only a single wireless access point **52** scans at any given time. When an access point is off-line for scanning, the wireless clients can immediately associate, without loss of connectivity, to an adjacent wireless access point **52**, if any, with the same SSID or within the same ESS (Extended Service Set).

After rogue AP scanning parameters are entered, airspace management platform **56**, in one embodiment, builds a job schedule. In one embodiment, all tasks are executed as jobs via the scheduler whether the job is scheduled for a later time or immediate/on-demand. In one embodiment, a task comprises a scan by a single wireless access point **52**; accordingly, a requested group scan may yield a plurality of jobs in the job scheduler. In one embodiment, when the job scheduler executes a job, it constructs an SNMP SET request and transmits it to the wireless access point **52** associated with the job. For example, in embodiments where wireless access point(s) **52** support(s) the SNMP MIB set forth in Appendix A, the job scheduler executes a SNMP SET request for Object Identifier (OID) (1.3.6.1.4.12028.4.3.4 BeginRogueAPScan) which, in one embodiment, passes the following value sets: {(packetsToCollect type-integer, value), (secsToWaitPerChan type-integer, value), (channelBeginScan, type-integer, value), (channelEndScan, type-integer, value), (channelToSkip, type-integer, value), and (numberOfIterations, type-integer, value)} [see Appendix A]. In one embodiment, airspace management platform **56** waits for a configurable number of seconds after the SNMP SET request to receive all device scan traps (scanDataRow) and the end of scan trap (endRogueScan) from the scanning access point **52**. If no traps are received, airspace management platform **56** transmits another SNMP SET request. If no traps are received after a threshold number of SET requests, airspace management platform **56** reports a fault condition to the network administrator.

B. Scanning Wireless Airspace

After receiving the SNMP-SET request from airspace management platform **56**, the wireless access point **52** invokes a locally executed scanning agent which moves its WLAN Network Interface Card (NIC) card from BSS master mode or normal AP mode, to a promiscuous RF monitoring mode. Many WLAN network interface cards installed on currently available wireless access points include promiscuous monitoring functionality, such as PrismII cards in LinkSys®, D-Link®, Compaq®, and Cisco® wireless access points. Promiscuous monitoring mode is a process that has analogy on the wired or wire line medium. On a wired network most Ethernet cards filter traffic so that only traffic destined for that card (installed in a PC or other network device) is received into higher layers of the operating system. Placing the LAN NIC card into "promiscuous mode" causes the LAN NIC to pass all traffic seen on the wire to higher layers in the operating system. On a non-switched or hub network, a computer or network device with its network card in promiscuous mode can listen to all traffic on the network segment. Similarly, in 802.11 or other wireless networks, the WLAN NIC, operating in its normal mode, only sends data packets destined for the device or management packets for Basic Service Set to higher layers in the operating system. In 802.11 wireless networks, wireless NICs, operating in a normal mode, only send packets within the same BSS and the same SSID to higher layers of the operating system. RF promiscuous mode, however, enables the wireless NIC to sniff all traffic in the surrounding airspace (radio coverage area and relative to one to a plurality of channels) regardless of network association.

FIG. **6** illustrates a method, according to an embodiment of the present invention, directed to scanning for rogue access points. When a designated wireless access point **52** receives an SNMP SET request (above) (**102**), a scanning agent changes the configuration of wireless access point **52** to operate in promiscuous RF monitoring mode (**104**). Once in this mode, the scanning agent executing within access point **52** uses the variables passed within the SNMP SET request to OID "beginRogueScan" to execute the properly formulated scan. Specifically, the scanning agent begins listening on the channel defined in the "channelBeginScan" variable (**106**). The scanning agent monitors this channel for packets and analyzes detected packets in order to build a memory array including data corresponding to detected wireless client devices and access points (**114**). In one embodiment, while a variety of packet types may be present, the scanning agent is configured to process only data packets and management-beacon packets to build the memory array of wireless devices, as discussed below. As FIG. **6** illustrates, the scanning agent listens on the current channel until it collects the number of packets defined in variable "packetsToCollect" (**110**) or until the channel timer has expired defined in variable "secsToWaitPerChan" (**112**). Next the scanning agent proceeds to the next channel (current channel+SNMP variable "channelToSkip") (**116**) until the next channel is greater than SNMP variable "channelEndScan" (**108**).

FIGS. **7**A (management) and **7**B (data) set forth the frame layout according to the 802.11 specification and illustrates how the scanning agent analyzes the data packets gathered while in the promiscuous monitoring mode to populate a memory array. FIG. **7**A illustrates the frame layout of a management packet, such as a beacon packet transmitted by an access point. As FIGS. **7**A and **7**B illustrate, packet type (e.g., data v. beacon) in the 802.11 standard can be determined by examining the values of the frame control bits. FIG. **7**A illustrates how the scanning agent can detect various fields such as BSSID, SSID, Channel and the like. Furthermore, FIG. **7**B illustrates the frame layouts of data packets transmitted from (top layout) and to (bottom layout) a wireless access point. As FIG. **7**B illustrates, the direction of data packets can be determined by evaluation of the values of the frame control bits. With the direction, the scanning agent can resolve whether the first address (address **1**) or the second address (address **2**) corresponds to the access point (BSSID). The RSSI (relative signal strength) is provided by a physical layer header called PrismII monitor header that is not a part of 802.11 frame header, but is generated by the firmware of the receiving card. One skilled in the art will recognize that other wireless protocol standards feature different frame layouts and will be able to configure the scanning agent to parse the various data fields in the packet or frame headers.

In addition, FIG. **8** illustrates a memory array (top table) including data obtained during a hypothetical scan for didactic purposes. For example, the first row of the memory array indicates that, on channel **1**, the scanning access point detected a data packet transmitted from/to a wireless client (see Type field) associated with an access point having a WLAN MAC address or BSSID of 00:02:2D:03:4C:B0. Further, the second row indicates that the scanning access point also detected a data packet from the same client on channel **2**. As one of skill in the art will recognize, the channels defined in the 802.11 specification only include 3 non-overlapping channels (**1**, **6** and **11**) among the total number of channels. As one of skill in the art understands, the channel represents the center frequency that the transceiver within the radio and access point uses (e.g., 2.412 GHz for channel **1** and 2.417 GHz for channel **2**). There is only 5 MHz separation between the center frequencies. Furthermore, an 802.11b signal occupies approximately 30 MHz of the frequency spectrum. The signal falls within about 15 MHz of each side of the center frequency. As a result, an 802.11b signal overlaps with several adjacent channel frequencies. This leaves only three channels (channels **1**, **6**, and **11** for the U.S.) that can be used without causing interference between access points. Accordingly, a scanning access point is likely to detect data packets from a given wireless client or access point on more than one channel. For example, scanning on channels **3** and **4**, the scanning access point **52**, in the didactic hypothetical, detected beacon packets from an access point having a MAC address of 00:02:2D:03:4C:B0 and configured with an SSID of "AirPort Network." As FIG. **8** shows, the scanning access point detected no wireless traffic on channel **8** during the scan.

As FIG. **6** further illustrates, after the scan and memory array construction, the scanning agent analyzes the memory array (**118**) and sends back a summarized set of traps to airspace management platform **56** (**120**). The table illustrated in FIG. **8** and entitled "Post Analysis Data Sent via SNMP to AMP from Scanning AP" illustrates the scanDataRow traps (each row corresponding to a trap). In one embodiment, the scanning agent resolves discrepancies such as the channels on which packets were detected in creating the scanDataRow traps. See also Appendix A ("scanDataRow"). As FIG. **8** illustrates, the scanning agent logically assigned the closest usable (non-overlapping) channel to the networks implemented by access points "00:03:2F:00:12:AE" and "00:02:2D:0D:4D:7C". Also notice the Access Point "00:02:2D:03:4C:B0" is summarized into a single trap event though it was heard on channel **3** and channel **4**. Because 802.11-compliant beacon frames identify the transmitting channel, the scanning agent assumes that the channel identified in the beacon packet (here, channel **1**) is correct and that the data packet detected during the scan on channel **4** bleed-over from channel **1**. In the example illustrated in FIG. **8**, at the end of the analysis, the scanning access point **52** would transmit to airspace management platform **56** four "scanDataRow" SNMP traps and one "endRogueAP" SNMP traps (signaling the end of the scan and indicating the number of scanDataRow traps sent).

As one skilled in the art will recognize, the scanning agent described above does not distinguish between registered/authorized wireless devices and rogue or non-registered devices. Rather, as discussed above, the data generated during the scan is summarized and sent as SNMP traps to airspace management platform **56**, which processes the traps (as discussed more fully below) to detect the present of rogue access points and/or wireless clients. One skilled in the art will recognize, however, that this division of functionality is not required by any constraint, and that the scanning agent executed by the access point(s) **52** can be configured to detect for the presence of rogue access points and transmit corresponding SNMP traps to airspace management platform **56**. A preferred embodiment, however, is the example described herein where the scanning agent running on the access point only collects data characterizing detected wireless traffic and transmits this collected data or summarized versions to airspace management platform **56** for further analysis. Airspace management platform **56**, according to a preferred embodiment, performs the analysis of the data, functioning as the SNMP manager while the access point functions as the agent in accordance with the principal foundations of the SNMP framework.

B.1. Identification of Access Points from SNMP Trap Data

Airspace management platform **56** receives the scanDataRow traps and processes them to identify rogue wireless devices. In one embodiment, each scanDataRow trap is processed against the information contained in one to a plurality of tables to identify rogue wireless devices operating within the airspace associated with the wireless network environment. In one embodiment, airspace management platform **56** maintains three categories of wireless devices: 1) authorized, 2) rogue, and 3) ignored. Authorized wireless access points are generally business grade access points (e.g., manufactured by Cisco, Lucent, Symbol, etc.) that have been authorized by the enterprise/network administrator and registered with airspace management platform **56** (see above). As discussed above, information relating to authorized access points is contained in the AP_Master table. As discussed more fully below, airspace management platform **56**, in one embodiment, also maintains a Rogue_Master table and an Ignored_Master table. An authorized wireless client or wireless station associates to an authorized access point and also possesses valid authentication credentials granted by a central security system. Rogue wireless devices encompass any wireless device (client or access point) in the enterprise's airspace that is not registered as an authorized or ignored device, as indexed by WLAN MAC address in the appropriate tables within the airspace management platform **56**. The ignored category represents wireless devices that have been processed through the rogue detection process set forth herein, reported to the network administrator and configured by the administrator in the Ignored category. An example would be an access point from a neighboring business. The access point is not rogue, but is nevertheless worthy of attention and is generally ignored until a change associated with the access point is detected.

Against this exemplary backdrop, each "scanDataRow" trap is processed in the following manner. Airspace management platform **56**, in one embodiment, evaluates the "awAPReturnBSSID" against the three categories of wireless devices (authorized, ignored and rogue) in the Master, Ignored and Rogue AP tables. FIG. **9** sets forth a method for processing scanDataRow traps according to an embodiment of the present invention. In one embodiment, airspace management platform **56** first queries the AP_Master table, searching for matches between the awAPReturnBSSID and the WLAN MACs of the AP records in that table (**204**). If there is a match, airspace management platform **56** builds a history record for the AP (**220**), showing that it was scanned by the AP defined in the value "awAPScanID" or LAN MAC address.

If there is not a match between the "awAPReturnBSSID" and the WLAN MACs of the AP_Master table records, then airspace management platform **56** determines whether the "awAPReturnBSSID" matches any records contained in the Rogue_Master (**208**) and Ignored_Master (**206**) tables. If the awAPReturnBSSID matches an entry in either table, airspace management platform **56** builds a history record for the matching access point as discussed above. If there is not a match in either the Rogue_Master or Ignored_Master tables, then the airspace management platform **56** creates a Rogue_Master record with an index using the WLAN MAC or "awAPReturnBSSID" (**210**). As FIG. **9** shows, airspace management platform **56** also builds a history record for the Rogue AP (**220**), showing that it was scanned by the AP defined in the value "awAPScanID" or the LAN MAC address.

In one embodiment, history records are maintained in a history table indexed by WLAN MAC address and further contain the remaining data elements contained in the scanDataRow trap. By building these relationships, airspace management platform **56** can analyze these history records to determine which authorized access points are contiguous, on what channel these APs are broadcasting, and the relative signal strength of their transmissions. Utilizing this information, airspace management platform **56** can automatically configure (or the network administrator can manually configure) the transmission power level and channel for optimum performance in light of the surrounding access points. For 802.11b as regulated in the United States in particular, there are only 3 non-overlapping channels (**1**, **6**, and **11**), so this high-level logic is extremely valuable and can be used to ensure that contiguous access points (those with overlapping airspaces) are configured to broadcast on non-overlapping channels. In a multi-floor environment a third dimension of height or floor level is added. Airspace management platform **56** seamlessly learns and links all access points by contiguous airspace by determining which access points can sense each other. As discussed above, the AP_Master record also stores the positional (e.g., GPS) coordinates associated with each wireless access point **52**, allowing a true 3-dimensional depiction of a WLAN environment. Currently produced access points do not generally contain GPS receivers, accordingly, the information recorded in the database is only as accurate as a human translating the GPS reading from a handheld device at the location of the access point, and inputting the information into the database of airspace management platform **56**. As one skilled in the art will recognize, the integration of GPS receivers into wireless network access points and corresponding MIB extensions to expose the GPS coordinates computed by the receiver can be readily accomplished. Accordingly, future embodiments of airspace management platform **56** also contemplate querying access points via SNMP or similar protocols for GPS coordinates. Even without GPS coordinates, airspace management platform **56** is still able to produce a 2-dimensional representation of the airspace associated with an administrative domain, mapping out contiguous access points.

B.2. Notifications

In one embodiment, an aspect of airspace management platform **56** is operative to provide notifications upon the detection of certain events (e.g., detection of a rogue access point, changes to ignored devices, changes/degradation of network performance characteristics, etc.). All data from access points, clients, security repositories, and network infrastructure is monitored on a real-time or near-real-time basis. Airspace management platform **56** further allows network administrators to define triggers when one or more collected data values exceed a threshold. Triggers cause an alert action to take place when the threshold is exceeded. Rogue access points, in one embodiment, fall under the security category. In one embodiment, there is a specific system trigger entitled "New Rogue AP Discovered" where a network administrator can define how he/she wants to receive immediate communication about the presence of a rogue device in the airspace. The three avenues for communication, in one embodiment, are email (address or distribution list), log (message is written into a syslog), and NMS (a trap is sent to a Network Management System like HP OpenView).

FIG. **9** illustrates that, in one embodiment, airspace management platform **56** issues a notification in response to the detection of rogue access points and/or changes to ignored access points. As described above, wireless devices discovered during a wireless scan of the airspace are categorized depending on airspace management platform **56** system settings (e.g., the state of the AP_Master and other tables) as Authorized, Ignored or Rogue. Specifically, as FIG. **9** shows, when airspace management platform **56** categorizes a wireless device as a rogue device (**208**, **210**), it issues a notification (**216**). Similarly, detected changes to an Ignored device (**214**) can also cause airspace management platform **56** to issue a notification. In one embodiment, The ignored_Master table contains a flag "AlertOnChange". If this flag is set (**212**), airspace management platform **56**, in one embodiment, compares the channel, SSID, and WEP of the Ignored access point in the Ignored_Master Table to the information received in the scanDataRow trap.

The Ignored device category, in one embodiment, can be used for access points that are not rogue access points connected to an enterprise's local area computer network, but for those access points that nevertheless overlap with the airspace associated with the enterprise's administrative domain. For example, this could be a legitimate, physically-adjacent enterprise's access point beyond the network administrator's control, but still worthy of monitoring. For example, the network administrator having knowledge of such an access point can engineer his network so that the access points **52** that overlap the airspace with the neighboring access point are operating on a different channel and SSID. The "AlertOnChange" flag, in one embodiment, indicates to airspace management platform **56** only to notify the network administrator when this Ignored device changes channel, SSID, or location, as these settings and the access point's location could impact the performance of the enterprise's wireless network. When the "AlertonChange" flag is set airspace management platform **56** looks at the trigger definition of "Ignored AP Alert on Change" and sends the appropriate notifications. As one skilled in the art will recognize, the detection of a new/unknown wireless device, according to the embodiments described above, will never directly create an entry into the Ignored_Master table. Rather, as FIG. **9** illustrates, the detection of an unknown wireless device creates a new entry into the Rogue_Master table and is reported to a network administrator. The network administrator can then decide whether to place the discovered wireless device in the Ignored category and, therefore, the Ignored_Master table.

In one embodiment, airspace management platform **56** allows network administrators to configure a "New Rogue AP Discovered" trigger defining how notifications are issued. Depending on the definition of "New Rogue AP Discovered" trigger, airspace management platform **56**, in one embodiment, creates a notification or notifications containing the following information: 1) LAN MAC and AP Name of discovering access point, 2) date and time the scan was initiated, 3) the duration of the scan, 4) the WLAN MAC of the Rogue device, 5) the SSID of the WLAN device, 6) the channel of the Rogue device, and 7) potentially the Client Radio MAC address. Included in each of these notifications, according to one embodiment, are URL links back to the Rogue Event, Discovering access point, and Rogue device. The URL link enables recipient network administrators immediate access over a computer network to resolve the rogue problem. FIG. **11** illustrates a user interface, according to an embodiment of the present invention, detailing the information characterizing a detected rogue access point.

C. Isolation of Rogue Access Points

Once the scan or scans are complete and all scanDataRow traps are processed, airspace management platform **56** is operative to display information characterizing the state of the enterprise's airspace. FIG. **10** shows a user interface displaying a list of rogue devices detected during a scan. This page allows WLAN administrators to view all Rogue access points discovered in the scan and take appropriate action with respect to them. As FIG. **10** illustrates, airspace management platform **56**, in one embodiment, summarizes the rogue device information and sorts them by discovered date and time. From this interface, a network administrator can identify the number of rogue devices in the airspace that require further attention. In one embodiment, airspace management platform **56** includes an OUI database, which is an Organizationally Unique Identifier or a 24 bit globally unique assigned number from IEEE. This database allows airspace management platform **56** to match the first three octets of the Rogue WLAN MAC address back to the original manufacturer. In one embodiment, airspace management platform **56** includes an extended OUI database that incorporates model numbers to the 4^{th} and 5^{th} octets and cross referenced wireless manufacturer OUIs to their resale entities. As FIG. **10** shows, additional columns from this view include AP Name, SSID, Channel, WEP, RSSI, Discovery Date and Time, and Discovery Agent or AP. As FIG. **10** shows, the AP Name is blank unless and until the network administrator configures a name for it.

The SSID column allows the network administrator to quickly ensure that the detected rogue access point is not conflicting with a SSID of an authorized access point within the airspace associated with the enterprise's wireless LAN as it could hijack legitimate users associated with the conflicting authorized access point. The channel field is self explanatory, but plays an additional role in the Rogue Detail View. The WEP column allows an administrator to determine how large a security breach the access point really is. If WEP is disabled then the access point could potentially be bridging the enterprise LAN to any person within the access point's radio coverage cell. The Relative Signal Strength (RSSI) column represents the signal strength identified from the discovering access point to the rogue device.

FIG. **11** sets forth a user interface providing a detailed view of information relating to a given rogue access point detected during the scan. To continue the process of examining the rogue device, an administrator may drill into the detail view by double clicking the MAC or the AP Name in the interface of FIG. **10**. If the AP Name is not known it will display "Unknown". The user interface provides a network administrator the opportunity to name the detected device. The table has indexes on the WLAN MAC and the LAN MAC of the rogue device so duplicate or blank AP names do not breach the integrity of the database. In the detail view the administrator has the ability to update the AP Name, GPS coordinates, and notes regarding the access point. The first pass at this view can be utilized to find all access points that were detected within the airspace(s) of the scanning access point(s) **52**. Either utilizing GPS or basic triangulation a network administrator with the information provided by airspace management platform **56** has a good estimate of the location of the rogue access point. The relative signal strength indicator value adds some granularity to the potential location of the device as a small RSSI value relative to one scanning access point indicates that it may be further away, while a larger RSSI value indicates that it may be closer to the scanning access point.

The administrator now can proceed to the approximate location of the detected rogue access point with a GPS Receiver and wireless scanning tool. When the access point is located, the network administrator can physically disable the access point (for access points located on the wired network), note location (for access points not connected to the wired network), or take any other appropriate action. Using the airspace management platform **56**, the network administrator can update as much information gathered about the rogue access point by assigning a Name and notes about whom and how the access point was installed. For example, the rogue device could be an access point from a neighboring business. In this instance the name and notes fields would reflect this information. After updating the data, the network administrator can delete the record corresponding to the rogue access point, leave it in the rogue category, or place it in the authorized category (if rogue detection is being used to discover new and authorized devices) or the ignored category. Ignoring or deleting the rogue device completes the isolation process work flow for the selected rogue device. The administrator can then continue working on analyzing the remaining devices on the list until all rogue devices are isolated.

The following provides a didactic example illustrating application of the present invention. One example of this scenario would be where a first business installs a wireless network at a remote facility. Subsequently, an adjacent entity decides to install a WLAN in its small office. This access point is not a rogue as it is not installed on the enterprise's network, but the enterprise would nevertheless want to know about it. The first time a Rogue Scan is run on the access point for that particular remote facility, the discovered access point associated with the adjacent business would be detected and recorded as a rogue device. The network administrator would be very interested in determining whether the rogue device runs on the same or overlapping frequency channels of authorized access points that detected the rogue device during the scan. This would aid the administrator in adjusting the configuration of, and optimizing the performance of, the enterprise's wireless network. The network administrator would also want to ensure that the adjacent access point is not configured with the same SSID. The network administrator may also desire to know whether WEP was enabled on the adjacent access point as any wireless client may associate to the rogue access point that does not have WEP enabled instead of the desired enterprise access point. Using airspace management platform **56**, the network administrator could quickly run a report to show usage patterns for the days preceding detection of the rogue device. If the number of users and wireless traffic has declined significantly, then the network administrator could travel to the remote location to determine the best means of resolution. If the user and traffic numbers have not declined, the network administrator could simply move the detected access point to the ignored classification with "alert on change" set. As the example illustrates, the present invention reduces the cost of monitoring the WLAN by (1) minimizing the time and resources required to roam throughout the enterprise with a laptop sniffing for rogue access points and users, by (2) allowing an enterprise to leverage a single device, or multiple devices, to function as an access point and air scanner, and (3) by centrally managing all access points from a single console.

Lastly, although the present invention has been described as operating in connection with wireless devices employing the 802.11b protocol, the present invention has application in a variety of computer network environments employing any suitable wireless physical and link layer protocols, such as 802.11a, 802.11b, 802.11g, MAC layer protocols 802.11d 802.11e 802.11h and 802.11i, and Radio Bands 2.4 GHz and 5 GHz. Further, although embodiments of the present invention have been described as operating in connection with SNMP, any suitable protocols can be used. In addition, although embodiments of the present invention have been described as operating in connection with a local area network, the present invention can be deployed across other computer networks, such as the Internet or other wide area networks. Accordingly, the present invention has been described with reference to specific embodiments. Other embodiments of the present invention will be apparent to one of ordinary skill in the art. It is, therefore, intended that the claims set forth below not be limited to the embodiments described above.

APPENDIX A - MIB

```
-- *******************************************************
-- MIB Definition
-- * SNMP Set request from AMP to AP that support AW MIB for Rogues
-- * (1.3.6.1.4.12028.4.3(awAPMIB).4(beginRogueScan Set Request)
-- *******************************************************
-- beginRogueScan   OBJECT IDENTIFIER ::= { awAPMIB 4 }
packetsToCollect OBJECT-TYPE
  SYNTAX      Integer
  MAX-ACCESS      read-write
  STATUS      current
  DESCRIPTION
    "The number of 802.11 packets to collect prior to moving channels"
  ::= { beginRogueScan 1 }
secsToWaitPerChan OBJECT-TYPE
  SYNTAX      Integer
  MAX-ACCESS      read-write
  STATUS      current
  DESCRIPTION
    "The number of seconds to listen on each channel"
  ::= {beginRogueScan 2 }
channelBeginScan OBJECT-TYPE
  SYNTAX      Integer
  MAX-ACCESS      read-write
  STATUS      current
  DESCRIPTION
    "Starting Channel for scan"
  ::= { beginRogueScan 3 }
channelEndScan OBJECT-TYPE
  SYNTAX      Integer
      MAX-ACCESS      read-write
  STATUS      current
  DESCRIPTION
      "Ending Channel for scan"
  ::= { beginRogueScan 4 }
channelToSkip OBJECT-TYPE
  SYNTAX      Integer
  MAX-ACCESS      read-write
  STATUS      current
  DESCRIPTION
      "The number of channel to skip for each scan.   5 would
      get 1,6,11 for 802.11b in US"
  ::= { beginRogueScan 5 }
numberOfIterations
  SYNTAX      Integer
  MAX-ACCESS      read-write
  STATUS      current
  DESCRIPTION
      "The number of iterations-meaning the AP would start
    @ channelBeginScan listening for packetsToCollect or
    secsToWaitPerChan and loop until channelEndScan for
    numberOfIterations iterations. The default value is
    1, 99 will cause the AP to full time scan until next
```

-continued

APPENDIX A - MIB

```
    beginRogueScan is received            "
  ::= { beginRogueScan 6 }
-- **********************************************************
-- * Rogue AP Data Traps generate by the AP and sent back to the AMP
-- * (1.3.6.1.4.12028.4.3(awAPMIB).5(per row of data found)
-- **********************************************************
-- scanDataAP        OBJECT IDENTIFIER ::= { awAPMIB 5 }
awAPScanID OBJECT-TYPE
  SYNTAX      MacAddress
  MAX-ACCESS      read-only
  STATUS      current
  DESCRIPTION
       "The LAN MAC Address of the AP Performing the SCAN"
  ::= { scanDataAP 2 }
awAPReturnBSSID OBJECT-TYPE
  SYNTAX      MacAddress
  MAX-ACCESS      read-only
  STATUS      current
  DESCRIPTION
       "The BSSID or Radio MAC of the Access Point discovered.
    Only present on APs"
  ::= { scanDataAP 3 }
awAPReturnSSID OBJECT-TYPE
  SYNTAX      DisplayString
  MAX-ACCESS      read-only
  STATUS      current
  DESCRIPTION
       "The SSID of the Access Point discovered."
  ::= { scanDataAP 4 }
awAPReturnChannel OBJECT-TYPE
  SYNTAX      INTEGER
  MAX-ACCESS      read-only
  STATUS      current
  DESCRIPTION
      "The Channel contained only in Beacon Packets.
    Program could guess by data packets collected
    on Channels 5, 6, & 7 one could surmise that
    the client is on channel 6."
  ::= { scanDataAP 5 }
awAPReturnWEPOn OBJECT-TYPE
  SYNTAX      INTEGER {(1) False, (2) True}
  MAX-ACCESS      read-only
  STATUS      current
  DESCRIPTION
      "1 indicates WEP is & 2 indicates WEP is on"
  ::= { scanDataAP 6 }
awAPReturnType OBJECT-TYPE
  SYNTAX      INTEGER {(1) AP,(2) Client,(3) Adhoc, (4) Bridge }
  MAX-ACCESS      read-only
  STATUS      current
  DESCRIPTION
      "Type of device picked up on scan"
  ::= { scanDataAP 7 }
awAPReturnRSSI OBJECT-TYPE
  SYNTAX      INTEGER
  MAX-ACCESS      read-only
  STATUS      current
  DESCRIPTION
      "Relative Signal Strength"
  ::= { scanDataAP 8 }
awAPReturnClMAC OBJECT-TYPE
  SYNTAX      MacAddress
  MAX-ACCESS      read-only
  STATUS      current
  DESCRIPTION
      "MAC address of client wireless NIC-only valid for
    client devices."
  ::= { scanDataAP 9 }
scanDataRow NOTIFICATION-TYPE
    OBJECTS { awAPScanId,
      awAPReturnBSSID,
        awAPReturnSSID,
        awAPReturnChannel,
    awAPReturnWepOn,
    awAPReturnType,
    awAPReturnRSSI
    awAPReturnClMAC}
```

-continued

APPENDIX A - MIB

```
  STATUS      current
  DESCRIPTION
   "This trap is sent for AP and client observed in the BSA."
  ::= { scanDataAP 1 }
-- **********************************************************
-- * SNMP trap from AP to AMP
-- * (1.3.6.1.4.12028.4.3(awAPMIB).6(endRogueScan Set Request)
-- **********************************************************
-- endRogueScan        OBJECT IDENTIFIER ::= { awAPMIB 6 }
awAPScanDuration OBJECT-TYPE
  SYNTAX      INTEGER
  MAX-ACCESS      read-only
  STATUS      current
  DESCRIPTION
    "Total duration of scan in seconds"
  ::= { endRogueDuration 2 }
awAPTotTraps OBJECT-TYPE
  SYNTAX      INTEGER
  MAX-ACCESS      read-only
  STATUS      current
  DESCRIPTION
    "Total traps(devices) sent to the AMP"
  ::= { endRogueDuration 3 }
endRogueScan NOTIFICATION-TYPE
    OBJECTS { awAPScanId,
      awAPScanDuration,
    awAPScanTotTraps}
  STATUS      current
  DESCRIPTION
   "This trap is sent for AP and client observed in the BSA."
  ::= { endRogueScan 1 }
```

What is claimed is:

1. A system facilitating the management of airspace associated with wireless computer network environments, comprising

an airspace management platform operably connected to a computer network, wherein the airspace management platform is operative to:

transmit requests for scans to wireless access points registered with the airspace management platform,

receive, from the wireless access points, scan data characterizing detected wireless traffic, and

analyze the data to identify rogue wireless devices; and

at least one wireless access point operably connected to the computer network,

wherein the at least one wireless access point includes wireless communications functionality allowing for wireless communication with at least one wireless client device;

wherein the at least one wireless access point further includes scanning functionality operative to detect wireless traffic on at least one frequency channel;

wherein the airspace management platform further comprises an ignored access point table including information relating to previously detected access points; and wherein the airspace management platform is operative to process scan data against the ignored access point table to identify rogue devices; and

wherein the at least one wireless access point comprises a scanning agent operative, in response to a request from the airspace management platform, to:

scan for wireless traffic;

record scan data characterizing the detected wireless traffic, and

transmit the scan data to the airspace management platform.

2. The system of claim **1** wherein the computer network is a local area computer network.

3. The system of claim **1** wherein the computer network is a wide area computer network.

4. The system of claim **1** wherein the scanning agent is operative to scan for wireless traffic on a plurality of frequency channels.

5. The system of claim **1** wherein the wireless traffic comprises a plurality of packets; and wherein the scanning agent is operative to parse the information in the packets, and transmit the packet information to the airspace management platform.

6. The system of claim **1** wherein that at least one wireless access point further comprises a management information base having an interface; and wherein the functionality of the scanning agent and the scan data is accessible through the interface.

7. The system of claim **6** wherein the interface is an SNMP interface.

8. The system of claim **7** wherein the at least one network access point is operative to transmit scan data in SNMP traps.

9. The system of claim **8** wherein scan data corresponding to a given detected device is transmitted in a separate SNMP trap.

10. The system of claim **8** wherein the airspace management platform is operative to process the SNMP traps to detect rogue devices.

11. The system of claim **1** wherein the airspace management platform comprises an access point table including information relating to registered access points; and wherein the airspace management platform is operative to process scan data against the access point table to identify rogue devices.

12. The system of claim **1** wherein the airspace management platform is operative to identify changes to an access point in the ignored access point table by comparing the scan data corresponding to the access point to the information in the ignored access point table.

13. The system of claim **12** wherein the airspace management platform is operative to issue a notification upon the detection of a change to an ignored access point.

14. The system of claim **1** wherein the airspace management platform is operative to issue a notification upon the detection of a rogue access point.

* * * * *

UNITED STATES PATENT AND TRADEMARK OFFICE

CERTIFICATE OF CORRECTION

PATENT NO. : 7,295,524 B1 Page 1 of 1
APPLICATION NO. : 10/368152
DATED : November 13, 2007
INVENTOR(S) : Gordon P. Gray et al.

It is certified that error appears in the above-identified patent and that said Letters Patent is hereby corrected as shown below:

On the Title page,

Item (75) Inventors: Delete "Daniel Thomas Augustino", and insert --Daniel Thomas Augustine--

Signed and Sealed this

First Day of April, 2008

Jon W. Dudas

JON W. DUDAS
Director of the United States Patent and Trademark Office

EXHIBIT B

US007376113B2

(12) **United States Patent**
Taylor et al.

(10) **Patent No.: US 7,376,113 B2**
(45) **Date of Patent: May 20, 2008**

(54) **MECHANISM FOR SECURELY EXTENDING A PRIVATE NETWORK**

(75) Inventors: **John Richard Taylor**, Tiburon, CA (US); **Pradeep J. Iyer**, Cupertino, CA (US); **Randy Chou**, San Jose, CA (US)

(73) Assignee: **Arubs Networks, Inc.**, Sunnyvale, CA (US)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 369 days.

(21) Appl. No.: **11/096,567**

(22) Filed: **Apr. 1, 2005**

(65) **Prior Publication Data**

US 2006/0221916 A1 Oct. 5, 2006

(51) **Int. Cl.**
H04Q 7/24 (2006.01)

(52) **U.S. Cl.** **370/338**; 370/299; 370/401; 370/467; 370/474; 370/476; 713/151; 713/160; 713/184

(58) **Field of Classification Search** 370/338, 370/299, 401, 465, 466, 474, 476; 455/410, 455/411; 709/227, 229, 230, 236, 238; 713/184, 713/151, 152, 160
See application file for complete search history.

(56) **References Cited**

U.S. PATENT DOCUMENTS

6,047,325	A *	4/2000	Jain et al.	709/227
6,708,218	B1 *	3/2004	Ellington, Jr. et al.	709/236
7,203,195	B2 *	4/2007	Hidaka et al.	370/392
2002/0015422	A1 *	2/2002	Inada et al.	370/474
2003/0039234	A1 *	2/2003	Sharma et al.	370/338
2003/0196105	A1 *	10/2003	Fineberg	713/200
2003/0231649	A1 *	12/2003	Awoseyi et al.	370/463
2006/0126659	A1 *	6/2006	Baum et al.	370/466

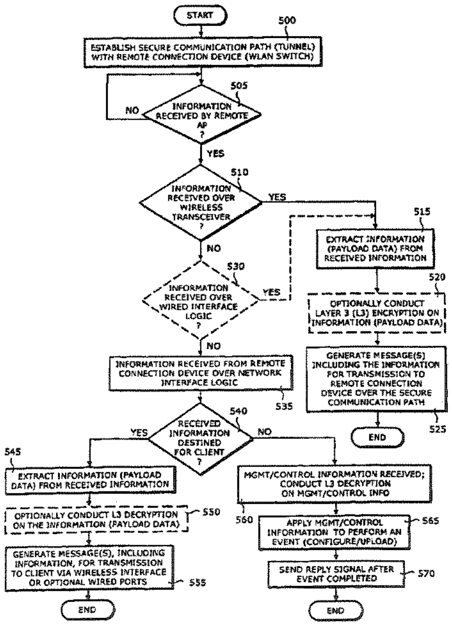
* cited by examiner

Primary Examiner—Matthew Anderson
Assistant Examiner—Shaima Q. Aminzay
(74) *Attorney, Agent, or Firm*—Blakely, Sokoloff, Taylor & Zafman

(57) **ABSTRACT**

According to one embodiment of the invention, a method for securely extending a private network to include one or more remote access points (APs) comprises a first operation of establishing a secure communication path with a destination device. Then, the information received from a source device is prepared for transmission to the destination device. This involves the received information undergoing Layer 3 (L3) encryption prior to encapsulation into a message for transmission to the destination device if the received information constitutes control information. If the received information constitutes data, the received information optionally undergoes L3 encryption, since the payload data might be already L2 encrypted by the source device, prior to encapsulation into the message.

12 Claims, 4 Drawing Sheets


START
500
ESTABLISH SECURE COMMUNICATION PATH (TUNNEL) WITH REMOTE CONNECTION DEVICE (WLAN SWITCH)
505
NO
INFORMATION RECEIVED BY REMOTE AP ?
YES
510
INFORMATION RECEIVED OVER WIRELESS TRANSCEIVER ?
YES
515
EXTRACT INFORMATION (PAYLOAD DATA) FROM RECEIVED INFORMATION
NO
530
INFORMATION RECEIVED OVER WIRED INTERFACE LOGIC ?
YES
520
OPTIONALLY CONDUCT LAYER 3 (L3) ENCRYPTION ON INFORMATION (PAYLOAD DATA)
NO
INFORMATION RECEIVED FROM REMOTE CONNECTION DEVICE OVER NETWORK INTERFACE LOGIC
GENERATE MESSAGE(S) INCLUDING THE INFORMATION FOR TRANSMISSION TO REMOTE CONNECTION DEVICE OVER THE SECURE COMMUNICATION PATH
535
540
YES
RECEIVED INFORMATION DESTINED FOR CLIENT ?
NO
END
525
545
EXTRACT INFORMATION (PAYLOAD DATA) FROM RECEIVED INFORMATION
MGMT/CONTROL INFORMATION RECEIVED; CONDUCT L3 DECRYPTION ON MGMT/CONTROL INFO
OPTIONALLY CONDUCT L3 DECRYPTION ON THE INFORMATION (PAYLOAD DATA)
550
560
APPLY MGMT/CONTROL INFORMATION TO PERFORM AN EVENT (CONFIGURE/UPLOAD)
565
GENERATE MESSAGE(S), INCLUDING INFORMATION, FOR TRANSMISSION TO CLIENT VIA WIRELESS INTERFACE OR OPTIONAL WIRED PORTS
555
SEND REPLY SIGNAL AFTER EVENT COMPLETED
570
END
END

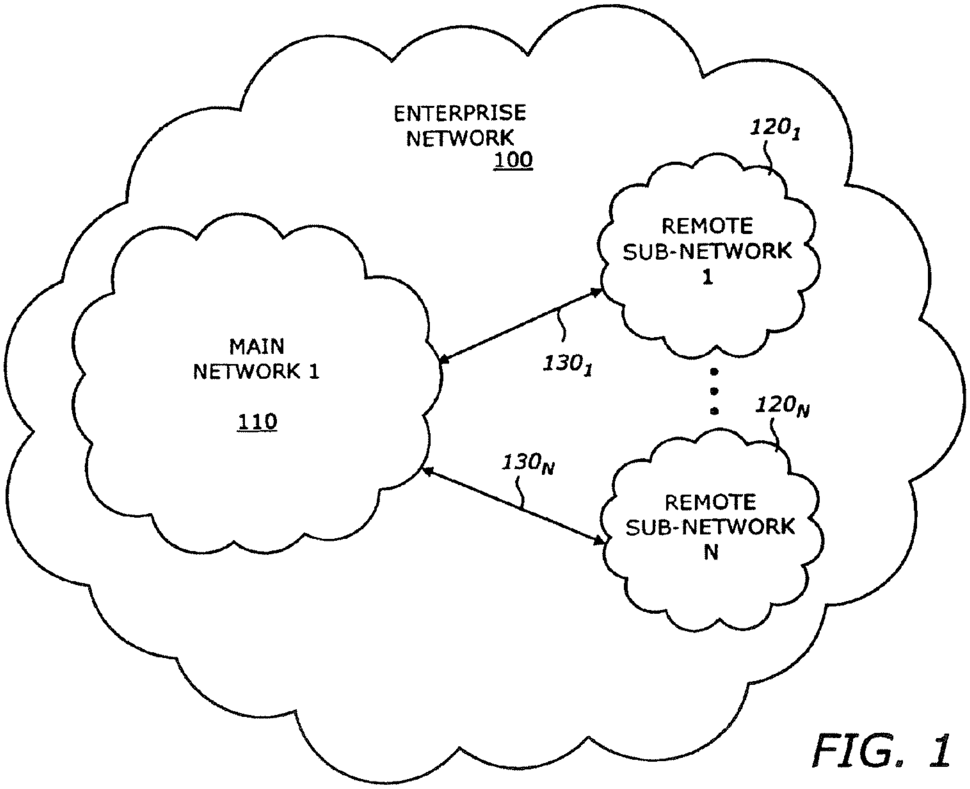

ENTERPRISE
NETWORK
100
120_1
REMOTE
SUB-NETWORK
1
MAIN
NETWORK 1
110
130_1
120_N
130_N
REMOTE
SUB-NETWORK
N

FIG. 1

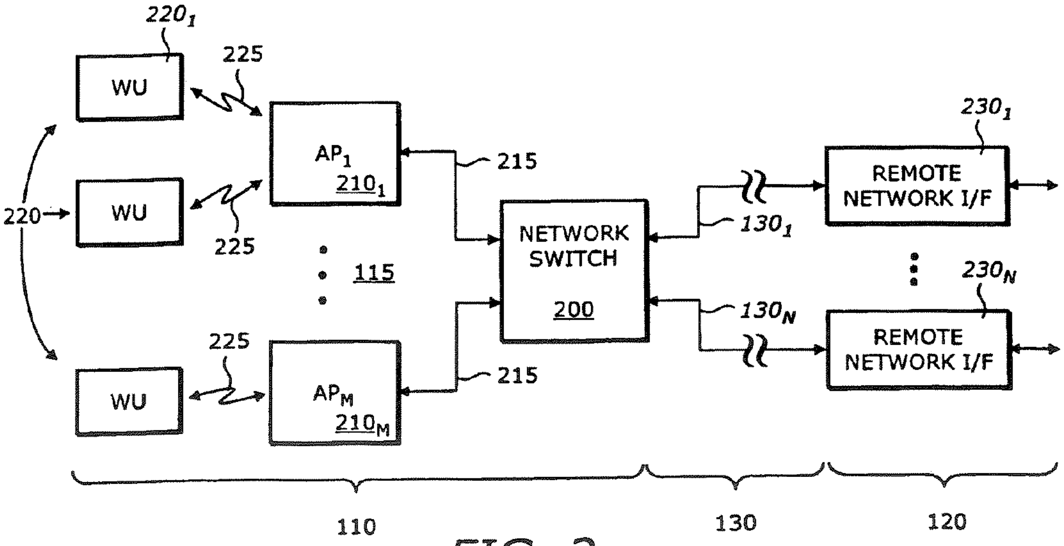

220_1
WU
225
AP_1
210_1
215
WU
220
225
115
NETWORK
SWITCH
200
230_1
REMOTE
NETWORK I/F
130_1
130_N
230_N
REMOTE
NETWORK I/F
225
WU
AP_M
210_M
215
110
130
120

FIG. 2

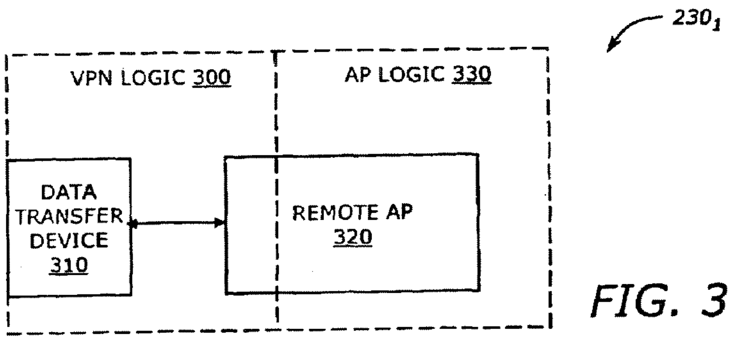


FIG. 3

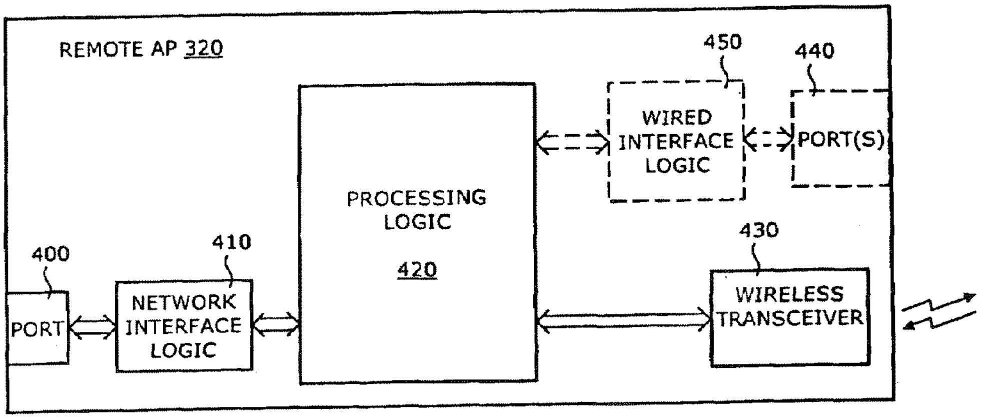


FIG. 4A

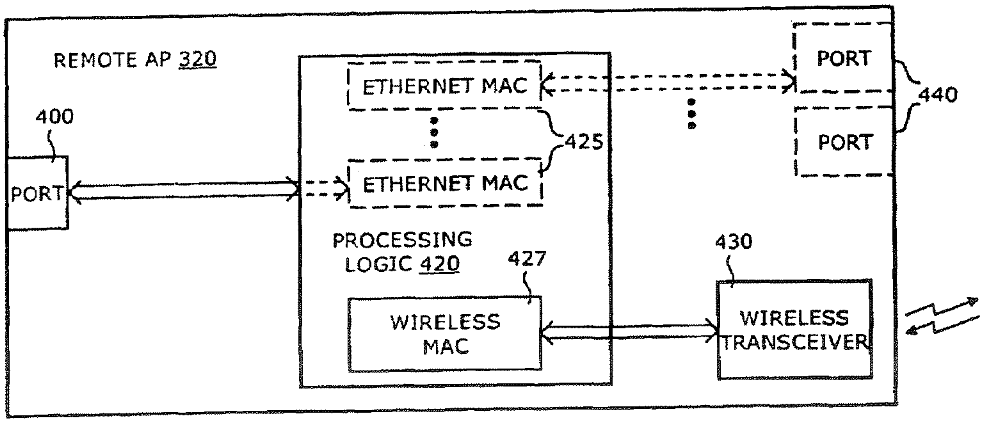


FIG. 4B

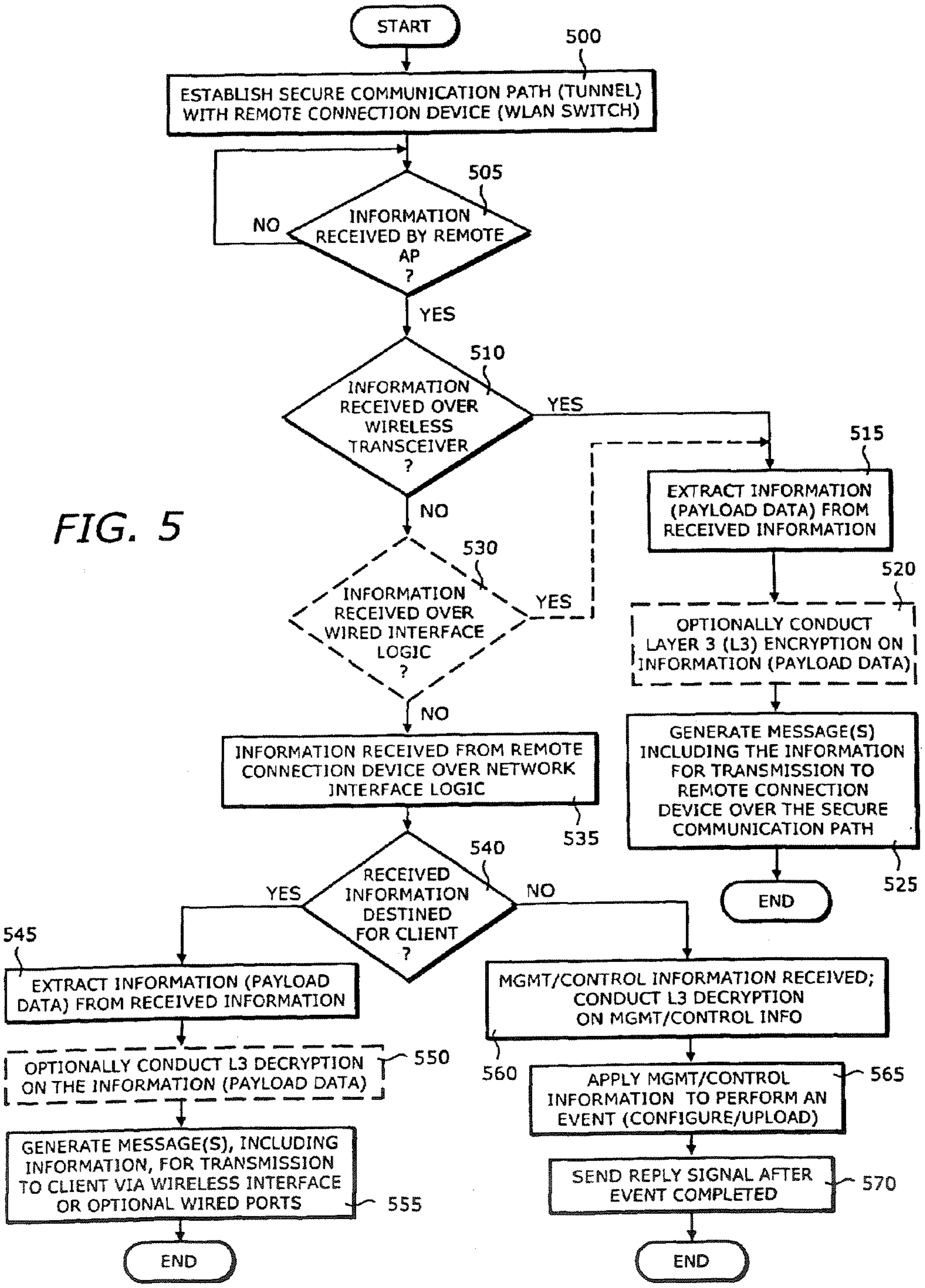

START
500
ESTABLISH SECURE COMMUNICATION PATH (TUNNEL) WITH REMOTE CONNECTION DEVICE (WLAN SWITCH)
505
NO
INFORMATION RECEIVED BY REMOTE AP ?
YES
510
INFORMATION RECEIVED OVER WIRELESS TRANSCEIVER ?
YES
515
EXTRACT INFORMATION (PAYLOAD DATA) FROM RECEIVED INFORMATION
520
OPTIONALLY CONDUCT LAYER 3 (L3) ENCRYPTION ON INFORMATION (PAYLOAD DATA)
GENERATE MESSAGE(S) INCLUDING THE INFORMATION FOR TRANSMISSION TO REMOTE CONNECTION DEVICE OVER THE SECURE COMMUNICATION PATH
525
END
NO
530
INFORMATION RECEIVED OVER WIRED INTERFACE LOGIC ?
YES
NO
INFORMATION RECEIVED FROM REMOTE CONNECTION DEVICE OVER NETWORK INTERFACE LOGIC
535
540
RECEIVED INFORMATION DESTINED FOR CLIENT ?
YES
NO
545
EXTRACT INFORMATION (PAYLOAD DATA) FROM RECEIVED INFORMATION
OPTIONALLY CONDUCT L3 DECRYPTION ON THE INFORMATION (PAYLOAD DATA)
550
GENERATE MESSAGE(S), INCLUDING INFORMATION, FOR TRANSMISSION TO CLIENT VIA WIRELESS INTERFACE OR OPTIONAL WIRED PORTS
555
END
MGMT/CONTROL INFORMATION RECEIVED; CONDUCT L3 DECRYPTION ON MGMT/CONTROL INFO
560
APPLY MGMT/CONTROL INFORMATION TO PERFORM AN EVENT (CONFIGURE/UPLOAD)
565
SEND REPLY SIGNAL AFTER EVENT COMPLETED
570
END

FIG. 5

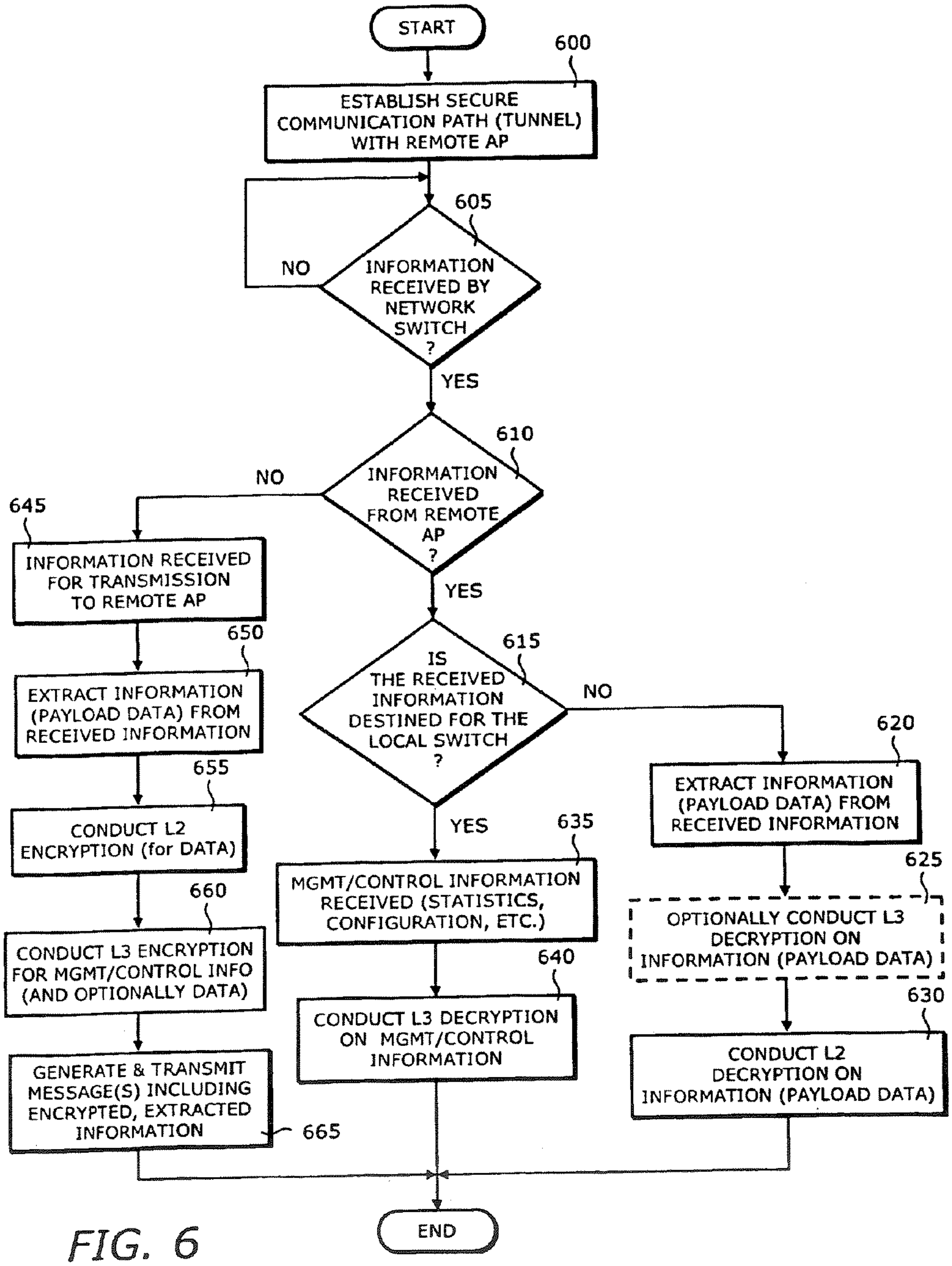

START
600
ESTABLISH SECURE COMMUNICATION PATH (TUNNEL) WITH REMOTE AP
605
INFORMATION RECEIVED BY NETWORK SWITCH ?
NO
YES
610
INFORMATION RECEIVED FROM REMOTE AP ?
NO
YES
645
INFORMATION RECEIVED FOR TRANSMISSION TO REMOTE AP
650
EXTRACT INFORMATION (PAYLOAD DATA) FROM RECEIVED INFORMATION
655
CONDUCT L2 ENCRYPTION (for DATA)
660
CONDUCT L3 ENCRYPTION FOR MGMT/CONTROL INFO (AND OPTIONALLY DATA)
GENERATE & TRANSMIT MESSAGE(S) INCLUDING ENCRYPTED, EXTRACTED INFORMATION
665
615
IS THE RECEIVED INFORMATION DESTINED FOR THE LOCAL SWITCH ?
NO
YES
635
MGMT/CONTROL INFORMATION RECEIVED (STATISTICS, CONFIGURATION, ETC.)
640
CONDUCT L3 DECRYPTION ON MGMT/CONTROL INFORMATION
620
EXTRACT INFORMATION (PAYLOAD DATA) FROM RECEIVED INFORMATION
625
OPTIONALLY CONDUCT L3 DECRYPTION ON INFORMATION (PAYLOAD DATA)
630
CONDUCT L2 DECRYPTION ON INFORMATION (PAYLOAD DATA)
END

FIG. 6

MECHANISM FOR SECURELY EXTENDING A PRIVATE NETWORK

FIELD

Embodiments of the invention relate to the field of wireless communications, in particular, to a system and apparatus for securely extending a private network to include one or more remote access points.

GENERAL BACKGROUND

Over the last decade or so, companies have installed enterprise networks with one or more local area networks in order to allow their employees access to various network resources. While these networks are typically configured to greatly improve work efficiency for employees physically at work, they tend to provide a lesser level of efficiency for those employees remotely accessing the enterprise network through a virtual private network (VPN).

For example, once a network is configured, employees become quite familiar with the manner in which resources of the network are accessed. This may involve increased familiarity with any graphic user interfaces as well as familiarity with association and authentication procedures. Employees working off-site, however, normally need to associate with different networks and navigate through various non-intuitive VPN client applications designed to form a VPN for accessing network resources from the enterprise network.

As a result, off-site employees access network resources less frequently, which may decrease productivity of these employees. In addition, off-site employees tend to use a greater amount of information technology (IT) resources than other employees, due in part to this lack of a uniform connectivity procedure.

SUMMARY

According to one embodiment of the invention, a method for securely extending a private network comprises (i) establishing a secure communication path with a destination device, and (ii) preparing information received from a source device for transmission to the destination device. The received information undergoes Layer **3** (L**3**) encryption prior to encapsulation into a message for transmission to the destination device if the received information constitutes control information, and optionally undergoing L**3** encryption prior to encapsulation into the message when the received information constitutes data. Moreover, the method further includes preparing information received from a remote connection device by (i) determining when the information received from the remote connection device is destined for a client device and (ii) conducting L**3** decryption on the information received from the remote connection device when the information received from the remote connection device is not destined for the client device. The information received from the remote connection device being either management or control information.

BRIEF DESCRIPTION OF THE DRAWINGS

The invention may best be understood by referring to the following description and accompanying drawings that are used to illustrate embodiments of the invention.

FIG. **1** is an exemplary embodiment of an extended network in accordance with the invention.

FIG. **2** is a detailed, exemplary embodiment of the network of FIG. **1**.

FIG. **3** is an exemplary generalized layout of a remote network interface unit of FIG. **2**.

FIG. **4**A is a first exemplary embodiment of the remote access point being a part of the remote network interface unit of FIG. **2**.

FIG. **4**B is a second exemplary embodiment of the remote access point being a part of the remote network interface unit of FIG. **2**.

FIG. **5** is an exemplary embodiment of a method of operation for a remote access point of FIGS. **4**A & **4**B.

FIG. **6** is an exemplary embodiment of a method of operation for the network switch of FIG. **2**.

DETAILED DESCRIPTION

Embodiments of the invention relate to a system and apparatus for securely extending a private network to include one or more remote access points (APs). According to one embodiment of the invention, a remote AP is configured to set up a secure tunnel to a remote connection device positioned physically inside a location with regulated occupancy (e.g., office, building, etc.). This "remote connection device" may be part of the private network, such as a network switch for example. One type of network switch is a wireless local area network (WLAN) switch if the network features wireless connectivity enhancements to operate as a wireless local area network (WLAN).

More specifically, the remote AP configuration is designed to seamlessly expand the private network (e.g., a WLAN) to the remote AP, allowing a client device to associate with the remote AP and authenticate with resources of the private network just as if the user was physically at the location. The remote AP may be adapted with a second network port to allow a user of the remote AP to alternatively connect to the private network via a wired medium.

In summary, according to one embodiment of the invention, the remote AP sets up a secure communication path by establishing a tunnel in accordance an Open Systems Interconnection (OSI) "Layer **3**" (L**3**) security protocol that protects and authenticates messages between participating devices. One type of L**3** security protocol is Internet Protocol Security (IPsec) protocol. For management and control information, IPsec cryptographic operations (e.g., encryption/decryption) are used. For transferred data, however, remote AP allows for optimized performance where no cryptographic operations are performed on the data transmitted through the tunnel. Rather, there is reliance on OSI "Layer **2**" (L**2**) encryption to provide sufficient obfuscation of the data without having to add additional computation complexity through Tripe Data Encryption Standard (3DES) or other encryption schemes.

Herein, according to one embodiment, the invention may be applicable to a variety of wireless networks such as a wireless local area network (WLAN) or wireless personal area network (WPAN). The wireless network may be configured in accordance with any current or future wireless communication protocols. Examples of various types of wireless communication protocols include Institute of Electrical and Electronics Engineers (IEEE) 802.11 standards, High Performance Radio Local Area Networks (HiperLAN) standards, WiMax (IEEE 802.16) and the like. For instance, the IEEE 802.11 standard may an IEEE 802.11b standard entitled "Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications: Higher-Speed Physical Layer Extension in the 2.4 GHz Band" (IEEE 802.11b, 1999); an IEEE 802.11a standard entitled "Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications: High-Speed Physical Layer in the 5 GHz Band" (IEEE 802.11a, 1999); a revised IEEE 802.11 standard "Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications" (IEEE 802.11, 1999); or an IEEE 802.11g standard entitled "Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications: Further Higher Data Rate Extension in the 2.4 GHz Band" (IEEE 802.11g, 2003).

Certain details are set forth below in order to provide a thorough understanding of various embodiments of the invention, albeit the invention may be practiced through many embodiments other that those illustrated. Well-known logic and operations are not set forth in detail in order to avoid unnecessarily obscuring this description.

In the following description, certain terminology is used to describe features of the invention. For example, "logic" includes hardware and/or software module(s) that are configured to perform one or more functions. For instance, a "processor" is logic that processes information. Examples of a processor include, but are not limited or restricted to a microprocessor, an application specific integrated circuit, a digital signal processor, a micro-controller, a finite state machine, or even combinatorial logic.

A "software module" is executable code such as an operating system, an application, an applet or even a routine. Software modules may be stored in any type of memory, namely suitable storage medium such as a programmable electronic circuit, a semiconductor memory device, a volatile memory (e.g., random access memory, etc.), a non-volatile memory (e.g., read-only memory, flash memory, a hard drive, etc.), a portable memory device (e.g., floppy diskette, a compact disk "CD", digital versatile disc "DVD", a tape, a Universal Serial Bus "USB" flash drive), or the like.

An "interconnect" is generally defined as a communication pathway established over an information-carrying medium. The interconnect may be a wired interconnect, where the medium is a physical medium (e.g., electrical wire, optical fiber, cable, bus traces, etc.) or a wireless interconnect (e.g., air in combination with wireless signaling technology).

"Information" is defined as data, address, control, management (e.g., statistics) or any combination thereof. For transmission, information may be transmitted as a message, namely a collection of bits in a predetermined format. Different types of messages include a packet, a frame or a cell, each including a header and payload data and having a predetermined number of bits of information.

I. General Network Architecture

Referring to FIG. **1**, an exemplary embodiment of an enterprise network **100** is shown. In accordance with one embodiment of the invention, a main network **110** operates as a private network, which includes at least one local area network. The local area network may be adapted with an enhancement that allows remote wireless access, thereby operating as a wireless local area network (WLAN).

One or more remote sub-networks $\mathbf{120}_1$-$\mathbf{120}_N$ (where $N \geqq 1$) are remotely located from main network **110** and are in communication via interconnect **130**. According to one embodiment of the invention, peer-to-peer communications are established between main network **110** and remote sub-networks $\mathbf{120}_1$-$\mathbf{120}_N$ via interconnects $\mathbf{130}_1$-$\mathbf{130}_N$, respectively. It is contemplated, however, that sub-networks $\mathbf{120}_1$-$\mathbf{120}_N$ may be in multicast communications with main network **110**.

Referring now to FIG. **2**, a detailed, exemplary embodiment of enterprise network **100** of FIG. **1** is illustrated. According to this embodiment of the invention, main network **110** features a WLAN **115** that comprises a network switch **200** (e.g., WLAN switch) in communication with one or more access points (APs) $\mathbf{210}_1$-$\mathbf{210}_M$ (where $M \geqq 1$) over an interconnect **215**. Interconnect **215** may be established using a wired or wireless information-carrying medium. In addition, one or more wireless units (WUs) **220** are in communication with APs $\mathbf{210}_1$-$\mathbf{210}_M$ over wireless interconnects **225**.

More specifically, each AP $\mathbf{210}_1$, . . . , or $\mathbf{210}_M$ supports bi-directional communications by receiving wireless messages from any or all of the WUs **220** within its coverage area and transferring data extracted from the messages over interconnect **215** to which network switch **200** is coupled.

WUs **220** are adapted to communicate with and access information from any associated AP. For instance, WU $\mathbf{220}_1$ is associated with AP $\mathbf{210}_1$ and communicates over the air in accordance with a selected wireless communications protocol. Hence, AP $\mathbf{210}_1$ generally operates as a transparent bridge connecting together a wireless and wired network.

According to one embodiment, WU $\mathbf{220}_1$ comprises a removable, wireless network interface card (NIC) that is separate from or employed within a wireless device that processes information (e.g., computer, personal digital assistant "PDA", telephone, alphanumeric pager, etc.). Normally, the NIC comprises a wireless transceiver, although it is contemplated that the NIC may feature only receive (RX) or transmit (TX) functionality such that only a receiver or transmitter is implemented.

Although not shown, interconnect **215** provides connectivity for network resources such as servers for data storage, web servers or the like. These network resources are available for users of main network **110**, albeit access may be restricted.

Network switch **200** comprises logic that supports bi-directional communications with APs $\mathbf{210}_1$-$\mathbf{210}_M$ over interconnect **215**. Namely, network switch **200** receives messages from and transmitting messages to one or more targeted APs $\mathbf{210}_1$, . . . , or $\mathbf{210}_M$ over interconnect **215**. According to one embodiment of the invention, interconnect **215** may be part of any type of wired network, including but not limited or restricted to Ethernet, Token Ring, Asynchronous Transfer Mode (ATM), or the like.

Network switch **200** is further adapted to perform L**2** & L**3** encryption and/or decryption operations on information transferred to or received from one or more remote network interfaces $\mathbf{230}_1$-$\mathbf{230}_N$. For instance, L**2** encryption is conducted on all data messages transmitted over interconnect **130**. L**3** encryption is optionally conducted for data messages if dual encryption is desired. However, L**3** encryption is conducted for all messages generated to route management or control information to the remote AP.

As shown in FIGS. **2** and **3**, each remote network interface, such as remote network interface $\mathbf{230}_1$ for this illustrative embodiment, includes VPN logic **300** and AP logic **330**. VPN logic **300** is used to establish a cryptographically secure communication path to a device, such as establishing an IPsec tunnel to network switch **200** within main network **110**. AP logic **330** is used to establish communications with a client device (not shown), which is physically distant from network switch **200**, but is utilized by an off-site user to gain access to WLAN **115**.

According to one embodiment of the invention, VPN logic **300** features a data transfer device **310** (e.g., a dial-up modem, a broadband modem, a modem/gateway combination) that, in cooperation with a various components of a remote AP **320**, establishes a cryptographically secure communication path (e.g., interconnect **130**$_1$) to network switch **200**. According to one embodiment of the invention, interconnect **130**$_1$ is a secure tunnel adapted to transfer information through one or more network address translation (NAT) devices to network switch **200**. The information is selectively encrypted and decrypted using any L3 cryptographic protocol such as IPsec, Secure Socket Layer (SSL) or other well-known or proprietary cryptographic protocol.

Other components of the remote AP **320**, which are represented as AP logic **330**, are used to establish a communication path with one or more client devices. Examples of "client devices" include wireless units or any other type of device that processes information (e.g., desktop computer, portable or laptop computer, personal digital assistant "PDA", etc.). The result provides seamless, secure access to main network **110** by the client device.

II. General Architecture of the Remote AP

Referring to FIG. **4**A, a first exemplary embodiment of remote AP **320** being a part of remote network interface unit **230**$_1$ of FIG. **2** is shown. Remote AP **320** comprises a first port **400**, network interface logic **410**, a processor **420** and a wireless transceiver **430**. As optional features, remote AP **320** may further comprise one or more additional ports **440** (e.g., a second port) and corresponding wired interface logic **450** to support wired communications with a client device in lieu of wireless communications over wireless transceiver **430**.

According to this embodiment, first port **400** is adapted for coupling with the data transfer device (not shown), and therefore, enables the receipt of messages from and the transmission of messages to the main network over interconnect **130**$_1$ of FIG. **2**. Network interface logic **410** is configured as a combination of hardware and software to control the transmission and receipt of information at the physical (PHY) and data link (MAC) layers (also referred to as "OSI Layer **1** and OSI Layer **2**").

More specifically, according to one embodiment of the invention, as shown in FIG. **4**B, network interface logic **410** may be adapted as an Ethernet controller embedded within processor **420** as shown. The Ethernet controller **410** provides Internet connectivity and operates to extract information from incoming messages, which is subsequently processed by other logic within processor **420** according to the operational flow set forth in FIG. **5**. The extracted information may include destination, source or intermediary addresses, payload data, management or control information, or the like. Similarly, Ethernet controller **410** is adapted to insert information into outgoing messages as well.

In lieu of an embedded implementation, it is contemplated that network interface logic (or Ethernet controller) **410** may be implemented as a separate integrated circuit with embedded network (Ethernet) functionality placed on a motherboard of remote AP **320**. Alternatively, such network (Ethernet) functionality may be achieved by configuring network interface logic (Ethernet controller) **410** as an expansion board that is coupled to the motherboard.

Wireless transceiver **430** comprises an antenna, a power amplifier, and other circuitry to support the radio functionality. More specifically, for one embodiment of the invention supporting IEEE 802.11 communication standards, wireless transceiver **430** comprises an antenna to receive incoming wireless messages. The wireless message(s) include IEEE 802.11 MAC frames encoded and carried within a frequency channel that is located within a carrier frequency band. The

carrier frequency band is located within typical radio frequency (RF) band of frequencies. For example, the RF band may generally fall within an approximate range of 2.4-2.5 GHz or perhaps an approximate range of 5-5.25 GHz. It is contemplated, though, that the invention may be applied to any frequency range.

Wireless transceiver **430** isolates the frequency channel on which data is carried from all the other frequencies received on the antenna. This may be accomplished through a tunable filter tuned to a center frequency of a channel of interest. The data channel undergoes a frequency shifting from the carrier band to baseband and the baseband analog radio signal is routed to an analog-to-digital converter (ADC). The ADC samples the baseband analog radio signal and converts it into digital information, which is transferred to processor **420** (e.g., wireless MAC **427**) and processed according to the operational flow set forth in FIG. **5**. In accordance with FIG. **4**B, the digital information may be used to produce messages for transmission via first port **400**.

As an optional feature, second port **440** and wired interface logic **450** may be adapted in remote AP **320** to support wired communications with the client device. As shown in FIG. **4**B, wired interface logic **450** may be implemented as an Ethernet MAC **425**, each associated with one or more ports, and thus, control PHY and MAC messaging as described above. This provides alternative coupling of the client device via wireless or wired interconnect.

III. General Operational Flow

A. Remote AP

Referring now to FIG. **5**, an exemplary embodiment of a method of operation for a remote AP implemented within a remote network interface **230**$_i$ (1≦i≦N) is shown. A secure communication path is established between the remote AP and a remotely located connection device such as network switch for example (block **500**).

Once the remote AP receives information, a determination is made whether the received information is one or more wireless messages from the wireless transceiver (blocks **505** and **510**). If so, at least a portion of the received information is extracted from the incoming wireless message(s) and inserted into one or more newly generated messages for transmission to the connection device (block **515** and **525**).

If the information to be transferred is management or control information, the extracted information is encrypted using IPsec or another L3 encryption scheme before insertion into the message(s) destined for the connection device. However, if the information constitutes data, the extracted information does not undergo L3 encryption because it might already be encrypted in accordance with L2 WLAN encryption. However, as an optional feature, if dual encryption is desired during network configuration, the payload data may be both L2 and L3 encrypted (block **520**).

If the remote AP does not receive information over the wireless transceiver, but instead receives the information from the wired interface logic received by the second port, the same operations set forth above will occur (blocks **515**-**530**). It is noted that payload data might already be encrypted in accordance with a selected L2 encryption scheme, and thus, further L3 encryption of payload data is optional.

In the event that the remote AP receives information, but does not receive information over the wireless transceiver or wired interface logic, the received information may have been received over the secure communication path (block **535**). Thereafter, a determination is made whether the received information is management or control information destined for the remote AP or data intended for the client device (block **540**).

If the received information is intended for the client device, the remote AP extracts a portion of the received information, such as the payload data for this example (block **545**). As an optional feature, the payload data may undergo L**3** decryption if the secure communication path (e.g. IPsec tunnel) is configured to conduct L**3** encryption on the payload data (block **550**). The payload data is inserted into an outgoing message for transmission to the client device (block **555**) located behind either the optional wired port(s) or the wireless interface.

When management or control, the extracted information is decrypted using IPsec or the chosen L**3** decryption scheme because such information always undergoes encryption prior to transmission through the secure communication path (block **560**). The management or control information is uploaded and perhaps processed to reconfigure the remote AP (block **565**). Upon successful performance of the desired event (e.g. reconfigure, upload, etc.), a reply signal is generated and returned to the connection device over the secure communication path (block **570**).

B. Network Switch

Referring to FIG. **6**, an exemplary embodiment of a method of operation for the network switch in communication with the remote AP is shown. A secure communication path is established with the remote AP (block **600**).

Once the network switch receives information, a determination is made whether the received information is from the remote AP or from an AP positioned locally within the private network (blocks **600**, **605** and **610**). If the received information is from the remote AP, as shown in block **615**, a secondary determination is made whether the received information is destined for either (1) the network switch itself, or (2) any other device except the network switch (e.g., a local AP or wireless unit).

If the received information is destined for a local AP or wireless unit, at least a portion of the received information (e.g., payload data) is extracted from the incoming message (s) and decrypted according to a selected L**2** decryption protocol (blocks **620** and **630**). As an optional feature, some of the extracted information may be decrypted according to a selected L**3** decryption protocol if dual encryption is conducted, namely L**3** encryption was conducted on the portion of the received information prior to transmission over the secure communication path (block **625**).

If the received information is management or control information, the extracted information is decrypted using IPsec or another L**3** encryption scheme before being processed (blocks **635** and **640**).

If the received information is not provided via the secure communication path, the information must have been received from any device in the main network **110** of FIG. **1**, such as a local AP where the information originated from a wireless unit in communication with the local AP (block **645**). Thereafter, at least a portion of the received information (e.g., payload data) is extracted from the incoming message(s) and is encrypted according to a selected L**2** encryption protocol (blocks **650** and **655**). If the extracted information is management or control information, the extracted information is encrypted according to a selected L**3** decryption protocol utilized by the secure communication path. Where dual encryption is desired for the payload data, as an optional feature, the payload data may undergoes an optional L**3** encryption operation prior to generating one or more messages for transmission over the secure communication path (block **660** and **665**).

While the invention has been described in terms of several embodiments, the invention should not limited to only those embodiments described, but can be practiced with modification and alteration within the spirit and scope of the appended claims. The description is thus to be regarded as illustrative instead of limiting.

What is claimed is:

1. A method comprising:

establishing a secure communication path with a destination device; and

preparing information received from a source device for transmission to the destination device, the received information (i) undergoing Layer **3** (L**3**) encryption prior to encapsulation into a message for transmission to the destination device if the received information constitutes control information, and (ii) optionally undergoing L**3** encryption prior to encapsulation into the message when the received information constitutes data; and

preparing information received from a remote connection device by (i) determining when the information received from the remote connection device is destined for a client device and (ii) conducting L**3** decryption on the information received from the remote connection device when the information received from the remote connection device is not destined for the client device, the information received from the remote connection device being either management or control information.

2. The method of claim **1**, wherein the destination device is the remote connection device being an Ethernet switch.

3. The method of claim **1**, wherein the preparing of the received information further undergoes L**3** encryption prior to encapsulation into the message when the received information constitutes management information.

4. The method of claim **1**, wherein the preparing of the received information constituting data is encapsulated without undergoing L**3** encryption since the data has undergone Layer **2** (L**2**) encryption by the source device.

5. The method of claim **1** further comprising

receiving information destined for the client device;

extracting a portion of the information;

optionally conducting L**3** decryption of the portion of information; and

generating a message including the portion of the information for transmission to the client device.

6. The method of claim **1**, wherein the L**3** encryption is in accordance with Internet Protocol Security (IPsec).

7. The method of claim **1**, wherein the preparing of information received from the remote communication device further comprises (iii) extracting and optionally conducting L**3** decryption on the information when the information received from the remote communication device is destined for the client device.

8. The method of claim **1** further comprising applying the management or control information to perform an event.

9. The method of claim **8** further comprising sending a reply signal after the event has been completed.

10. In communication with a remote connection device, a remote network interface comprising:

a data transfer device; and

a remote access point adapted to operate with the data transfer device to establish a secure communication path in accordance a Layer **3** (L**3**) security protocol with the remote connection device, the remote access point being configured to perform L**3** cryptographic operations on received management information and control information and configured to optionally perform L**3** cryptographic operations on received data, the remote access point comprises:

a wireless transceiver adapted to support communications with a client device,

at least one wired port adapted to alternatively support communications with the client device,

a port adapted to support communications with the remote connection device, and

a processor coupled to the wireless transceiver, the at least one wired port and the port, processor including (i) a plurality of Ethernet media access controllers

(MACs), each of the Ethernet MACs uniquely coupled to one of a group including the port and the at least one wired port, and (ii) a wireless MAC coupled to the wireless transceiver.

11. The remote network interface of claim **10**, wherein the data transfer device is a modem.

12. The remote network interface of claim **10**, wherein the remote access point configured to perform L**3** cryptographic operations on the received management information and control information and refraining from performing L**3** cryptographic operations on received data when the data is already Layer **2** (L**2**) encrypted.

* * * * *

EXHIBIT B

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF DELAWARE

SYMBOL TECHNOLOGIES, INC., a Delaware Corporation, and WIRELESS VALLEY COMMUNICATIONS, INC., a Delaware Corporation,

Plaintiffs~~ and Counter-Defendants~~,

v.

ARUBA NETWORKS, INC., a Delaware ~~corporation~~Corporation,

Defendant~~ and Counter-Claimant.~~,

C. A. No. 07-519-JJF

DEMAND FOR JURY TRIAL

ARUBA NETWORKS, INC., a Delaware Corporation

Counter-Claim Plaintiff,

v.

MOTOROLA, INC., a Delaware Corporation, SYMBOL TECHNOLOGIES, INC., a Delaware Corporation, and WIRELESS VALLEY COMMUNICATIONS, INC., a Delaware Corporation,

Counter-Claim Defendants.

~~FIRST~~

ARUBA NETWORKS, INC.'S SECOND AMENDED ANSWER AND COUNTERCLAIMS

~~INTRODUCTION AND SUMMARY~~

~~Sometimes, when companies are losing in the marketplace, they sue—hoping that they can persuade jurors to overrule the verdict of the market. This lawsuit, filed by Symbol~~

~~Technologies, Inc., and Wireless Valley Communications, Inc. (both wholly owned subsidiaries of global behemoth Motorola, Inc.), is that type of case.~~

~~Aruba Networks, Inc., was founded in 2002. In early 2003, it announced major advancements in wireless LAN technologies. Aruba's advancements allowed corporations and other enterprises to lock the air against intruders, enable high-speed mobile firewalls that follow users, and construct self-calibrating Wi-Fi networks. Aruba's innovations were met with widespread acclaim—and, almost immediately, Symbol's strong interest.~~

~~Recognizing the superiority of Aruba's technologies, Symbol tried to get access to them by buying Aruba. Throughout the first half of 2003, in the course of discussions initiated by Symbol, Aruba gave Symbol essentially unfettered access to Aruba's products—the way they were designed, built, tested, and made—and to Aruba's business and marketing strategies and plans. Although Symbol was very interested in acquiring Aruba and its technologies, ultimately the parties were not able to agree on the complete terms of a transaction.~~

~~In the years since Symbol's close inspection of Aruba, Aruba has continued to receive widespread recognition as a fast-growing technology innovator. In 2003, Aruba won the prestigious Comdex Best in Show Award. In 2005, it won the Techworld.com Wireless Security Product of the Year Award. In 2007, Aruba won the Best Wireless Broadband Security Innovation Award at the Wireless Broadband Innovations Awards, as well as the Best of Interop 2007: Wireless & Mobility Category. These are just a few of the many awards it has won since its founding in 2002.~~

~~Aruba's technological innovations have paralleled its success in the marketplace. For example, according to a published report by Dell'Oro Group, Aruba's share of the enterprise wireless LAN market rose to greater than 10% in the second quarter of 2007 from roughly 5% in the same period of 2005. During the same period, Motorola's Symbol unit lost market share, and Aruba displaced Motorola/Symbol as the world's second largest enterprise wireless LAN supplier.~~

~~On the eve of Aruba's quarterly earnings announcement a month or so ago, in which Aruba announced a significant increase in revenue, Motorola's subsidiaries, Symbol and Wireless Valley, filed this lawsuit — on patents that began issuing in 2003. The next morning, coincident with Aruba's earnings release and only hours in advance of Aruba's conference call, Motorola issued a press release announcing the filing of the suit. The complaint fails to explain why the plaintiffs:~~

- ~~waited for four years after Symbol's close inspection of Aruba's technology and business to sue;~~
- ~~sued with no prior notice to Aruba; and~~
- ~~chose to bring this lawsuit on the eve of Aruba's earnings announcement.~~

~~That explanation can be found in Aruba's success in the marketplace.~~

PARTIES

1. Aruba admits that in Securities and Exchange Commission filings Motorola, Inc., has described Symbol as a wholly owned subsidiary. Aruba is without knowledge or information sufficient to form a belief as to the truth of the remaining allegations of Paragraph 1 of the Complaint and therefore denies those allegations.

2. Aruba admits that in Securities and Exchange Commission filings Motorola, Inc., has described Wireless Valley as a wholly owned subsidiary. Aruba is without knowledge or information sufficient to form a belief as to the truth of the remaining allegations of Paragraph 2 of the Complaint and therefore denies those allegations.

3. Aruba admits that it is a Delaware corporation with a principal place of business at 1344 Crossman Avenue, Sunnyvale, CA 94089-1113, and that, for purposes of this action, The Corporation Trust Company is its registered agent for service of process in Delaware. The Complaint does not make clear what plaintiffs mean in the third sentence of Paragraph 3 of the Complaint, and Aruba therefore denies those allegations.

JURISDICTION AND VENUE

4. Aruba admits that this action purports to arise under the Patent Laws of the United States, Title 35, United States Code, but denies any wrongdoing or liability. Aruba further admits that this Court has subject matter jurisdiction over the allegations in the Complaint under 28 U.S.C. §§ 1331 and 1338(a).

5. Aruba does not dispute that for purposes of this action venue is proper in this judicial district.

6. Aruba admits that it is subject to personal jurisdiction in this judicial district because Aruba is a Delaware corporation with an agent for service of process in Delaware. Except as expressly admitted, Aruba denies the allegations of Paragraph 6 of the Complaint.

THE ASSERTED PATENTS – DENIAL OF INFRINGEMENT

7. Aruba admits that U.S. Patent No. 7,173,922 ("the '922 patent"), entitled "Multiple Wireless Local Area Networks Occupying Overlapping Physical Spaces," purports to have issued on February 6, 2007, but denies that this patent was duly and legally issued. Aruba admits that a document that purports to be a copy of the '922 patent is attached to the Complaint as Exhibit A, but Aruba lacks knowledge that it is a true and correct copy and therefore denies the remaining allegations of Paragraph 7 of the Complaint.

8. Aruba admits that U.S. Patent No. 7,173,923 ("the '923 patent"), entitled "Security In Multiple Wireless Local Area Networks," purports to have issued on February 6, 2007, but denies that this patent was duly and legally issued. Aruba admits that a document that purports to be a copy of the '923 patent is attached to the Complaint as Exhibit B, but Aruba lacks knowledge that it is a true and correct copy and therefore denies the remaining allegations of Paragraph 8 of the Complaint.

9. Aruba is without knowledge or information sufficient to form a belief as to the truth of the allegations of Paragraph 9 of the Complaint and therefore denies those allegations.

10. Aruba admits that U.S. Patent No. 6,625,454 ("the '454 patent"), entitled "Method and System for Designing or Deploying a Communications Network Which Considers

Frequency Dependent Effects," purports to have issued on September 23, 2003, but denies that this patent was duly and legally issued. Aruba admits that a document that purports to be a copy of the '454 patent is attached to the Complaint as Exhibit C, but Aruba lacks knowledge that it is a true and correct copy and therefore denies the remaining allegations of Paragraph 10 of the Complaint.

11. Aruba admits that U.S. Patent No. 6,973,622 ("the '622 patent"), entitled "System and Method for Design, Tracking, Measurement, Prediction and Optimization of Data Communication Networks," purports to have issued on December 6, 2005, but denies that this patent was duly and legally issued. Aruba admits that a document that purports to be a copy of the '622 patent is attached to the Complaint as Exhibit D, but Aruba lacks knowledge that it is a true and correct copy and therefore denies the remaining allegations of Paragraph 11 of the Complaint.

12. Aruba is without knowledge or information sufficient to form a belief as to the truth of the allegations of Paragraph 12 of the Complaint and therefore denies those allegations.

FIRST ASSERTED CLAIM – '922 PATENT

13. Aruba incorporates its responses to the allegations of Paragraphs 1-12 of the Complaint here.

14. Aruba denies the allegations of Paragraph 14 of the Complaint.

15. Aruba denies the allegations of Paragraph 15 of the Complaint.

16. Aruba denies the allegations of Paragraph 16 of the Complaint.

17. Aruba denies the allegations of Paragraph 17 of the Complaint.

18. Aruba denies the allegations of Paragraph 18 of the Complaint.

SECOND ASSERTED CLAIM – '923 PATENT

19. Aruba incorporates its responses to the allegations of Paragraphs 1-12 of the Complaint here.

20. Aruba denies the allegations of Paragraph 20 of the Complaint.

21. Aruba denies the allegations of Paragraph 21 of the Complaint.

22. Aruba denies the allegations of Paragraph 22 of the Complaint.

23. Aruba denies the allegations of Paragraph 23 of the Complaint.

24. Aruba denies the allegations of Paragraph 24 of the Complaint.

THIRD ASSERTED CLAIM – '454 PATENT

25. Aruba incorporates its responses to the allegations of Paragraphs 1-12 of the Complaint here.

26. Aruba denies the allegations of Paragraph 26 of the Complaint.

27. Aruba denies the allegations of Paragraph 27 of the Complaint.

28. Aruba denies the allegations of Paragraph 28 of the Complaint.

29. Aruba denies the allegations of Paragraph 29 of the Complaint.

30. Aruba denies the allegations of Paragraph 30 of the Complaint.

FOURTH ASSERTED CLAIM – '622 PATENT

31. Aruba incorporates its responses to the allegations of Paragraphs 1-12 of the Complaint here.

32. Aruba denies the allegations of Paragraph 32 of the Complaint.

33. Aruba denies the allegations of Paragraph 33 of the Complaint.

34. Aruba denies the allegations of Paragraph 34 of the Complaint.

35. Aruba denies the allegations of Paragraph 35 of the Complaint.

36. Aruba denies the allegations of Paragraph 36 of the Complaint.

SEPARATE DEFENSES

37. In addition to the defenses described below, Aruba expressly reserves the right to allege additional defenses as they become known through the course of discovery.

FIRST DEFENSE – NON-INFRINGEMENT

38. Aruba has not infringed, directly or indirectly, any valid asserted claim of the '922, '923, '454, or '622 patents (collectively "patents-in-suit").

SECOND DEFENSE – INVALIDITY UNDER §§ 102 AND 103

39. Aruba is informed and believes, and on that basis alleges, that each of asserted claims of each of the patents-in-suit is invalid for failure to meet the conditions of patentability set forth in 35 U.S.C. §§ 102 and 103, because the alleged inventions thereof are anticipated by, taught by, suggested by, and/or obvious in view of the prior art, and no claim of any of the patents-in-suit can be validly construed to cover any Aruba product or method.

THIRD DEFENSE – INVALIDITY UNDER § 112

40. Aruba is informed and believes, and on that basis alleges, that each of the asserted claims of each of the patents-in-suit are invalid for failure to comply with 35 U.S.C. § 112.

FOURTH DEFENSE – INVALIDITY UNDER § 101

41. Aruba is informed and believes, and on that basis alleges, that each of the asserted process claims of each of the patents-in-suit are invalid for failure to comply with 35 U.S.C. § 101.

FIFTH DEFENSE – EQUITABLE ESTOPPEL

42. The relief sought by Symbol is barred in whole or in part by the doctrine of equitable estoppel.

43. Without limiting the generality of the above allegations, Symbol asserts infringement because "Aruba designs, manufactures, and sells in the United States wireless switches (which it calls mobility controllers), access points, management servers, and related software for use in connection with WLANs, as well as software for designing, planning, configuring, monitoring, managing, and optimizing WLANs." (Complaint ¶ 3.)

44. Symbol has known this since at least early 2003, when it told Aruba that it (Symbol) wanted to purchase Aruba and spent months trying to convince Aruba to allow Symbol to purchase it. In the course of those efforts, Symbol sent senior engineers – ***including the individual named as the inventor on the '922 and '923 patents-in-suit*** – to Aruba to learn, in copious detail, about Aruba's products. Those discussions lasted for several months. During them, Aruba provided Symbol with extensive access to information about Aruba's products, the

way they were designed and built, the way they worked, Aruba's plans for manufacturing and selling them, and Aruba's plans for future products.

45. Although Symbol was very interested in acquiring Aruba and its technologies, ultimately the parties were not able to agree on the complete terms of a transaction.

46. At the time that Symbol was trying to convince Aruba to be purchased, Symbol's '922 and '923 patent applications were no longer confidential – they had been published two years earlier, in 2001. Although those Symbol patent applications were no longer confidential, at no point during Symbol's efforts to convince Aruba did Symbol advise or suggest that if Aruba did not agree to a transaction, Symbol would later assert those pending patents against it. At no point during Symbol's efforts to convince Aruba did Symbol advise or suggest that Symbol had already invented the technology that Aruba had. In fact, quite the contrary: Symbol was very impressed with Aruba's technologies, and told Aruba that it (Symbol) thought those technologies to be superior to, and different from, Symbol's.

47. Symbol's failures and omissions were particularly egregious given that the putative named inventor on those patent applications was an integral part of the senior engineering team that was handpicked by Symbol to learn about Aruba's products – the products that Symbol now says infringes the '922 and '923 patents, and have (according to Symbol) done so since 2003.

48. Symbol's failures and omissions led Aruba reasonably to infer that Symbol did not intend to enforce any patent rights, including the then-pending '922 and '923 patent applications if they issued as patents, against Aruba. As far as Aruba understood from Symbol's conduct and silence, the parties were going to go compete in the market and let the marketplace decide which technologies and businesses were superior.

49. Since its discussions with Symbol ended in 2003, Aruba has successfully continued its efforts to invest and to innovate. It has established customer relationships based on the products that it disclosed to Symbol during the discussions in 2003. It has spent tens of millions of dollars growing its business based on the products that it disclosed to Symbol in

2003. It has attracted key executive, engineering, finance, and sales personnel based on the success of the products that it disclosed to Symbol in 2003. In these and other ways, it would materially prejudice Aruba for Symbol to be allowed to proceed with its claims.

SIXTH DEFENSE – LACHES

50. The relief sought by Symbol and Wireless Valley is barred in whole or in part by the doctrine of laches. Aruba incorporates the allegations of Paragraphs 43 through 49 here.

51. Without limiting the generality of the above allegations, as noted above, Symbol and Wireless Valley assert infringement because "Aruba designs, manufactures, and sells in the United States wireless switches (which it calls mobility controllers), access points, management servers, and related software for use in connection with WLANs, as well as software for designing, planning, configuring, monitoring, managing, and optimizing WLANs." (Complaint ¶ 3.) Even leaving aside the 2003 discussions between Symbol and Aruba, Symbol and Wireless Valley have known of Aruba and its activities for years.

52. In May 2003, for example, industry press reported, in an article that quotes both Aruba and Symbol officials, that "Start-ups and old timers in the networking and wireless worlds are flocking to the wireless switching market. The list includes . . . Aruba Wireless Networks, . . . Symbol Technologies, [and others]." There are many other such press and other such examples. Accordingly, Symbol and Wireless Valley knew or reasonably should have known of the activities now alleged by Symbol and Wireless Valley to infringe the patents-in-suit long ago.

53. In fact, this is true ***even according to Symbol and Wireless Valley***. In an August 2007 industry article about this lawsuit, Symbol's current General Counsel is described as stating that "[a]ll of Aruba's WLAN switch, site planning and radio-frequency management and monitoring products infringe the patents, ***and they have since the company began selling its first products.***" Nevertheless, Symbol and Wireless Valley delayed in bringing this suit until August 2007, on patents that first started issuing in September 2003 – waiting while Aruba invested tens of millions of dollars in designing and testing its products, developing customer

relationships, and building its business. Symbol's and Wireless Valley's delay was unreasonable, inexcusable, and prejudicial to Aruba, and Symbol's and Wireless Valley's claims are barred as a result.

SEVENTH DEFENSE – INEQUITABLE CONDUCT ('922 AND '923 PATENTS)

54. Aruba is informed and believes, and on that basis alleges, that individuals charged with a duty of candor on behalf of Symbol failed, with an intent to deceive, to properly disclose to the U.S. Patent and Trademark Office information material to the patentablity of the '922 and '923 patents and failed to follow the requirements of the Manual of Patent Examiners Procedure necessary to have this information considered by the U.S. Patent and Trademark Office.

55. This information includes, but is not limited to, the existence of co-pending U.S. application no. 09/457,624 (the "'624 application"), filed on December 8, 1999. At the time of filing, the '624 application was purportedly owned by Proxim, Inc., and described and claimed subject matter that, to a reasonable patent examiner, would have been material to the patentability of the '922 and '923 patents. On or before October 1, 2004, Proxim assigned its rights in the '624 application to Symbol, so Symbol had knowledge of the contents of the '624 application at least as of the date of the assignment and likely before that. Despite knowing of the highly material contents of the '624 application, individuals charged with a duty of candor on behalf of Symbol failed to disclose the existence of the '624 application to the patent examiner responsible for the examination of the applications that resulted in the '922 and '923 patents. The patent examiner responsible for those applications would have found the 624 application material because, among other things, the examiner would have then been able to determine whether to issue a provisional obviousness-type double patenting rejection.

56. In light of the above, the '922 and '923 patents are not enforceable due to inequitable conduct.

EIGHTH DEFENSE – INEQUITABLE CONDUCT ('454 PATENT)

57. Aruba is informed and believes, and on that basis alleges, that individuals charged with a duty of candor on behalf of Wireless Valley failed, with an intent to deceive, to properly

disclose to the U.S. Patent and Trademark Office information material to the patentablity of the ’454 patent and failed to follow the requirements of the Manual of Patent Examiners Procedure necessary to have this information considered by the U.S. Patent and Trademark Office.

58. This information includes, but is not limited to, the following: (i) information and publications relating to SMT Plus, a software tool developed, at least in part, by Theodore Rappaport and Roger Skidmore, and licensed to over twenty entities more than one year prior to the filing date of the ’454 patent; (ii) the following publications, which the named inventors and/or prosecuting patent attorneys knew were never considered by the U.S. Patent and Trademark Office due to Wireless Valley’s late submission of an Information Disclosure Statement in violation of U.S. Patent and Trademark Office rules: R.P. Torres, et al., *CINDOOR: An Engineering Tool for Planning and Design of Wireless Systems in Enclosed Spaces*, IEEE Antennas and Propagation Magazine, Vol. 41, No. 4 (Aug. 1999); M. Panjwani et al., *Interactive Computation of Coverage Regions for Wireless Communication in Multifloored Indoor Environments*, IEEE Journal on Selected Areas in Communications, Vol. 14, No. 3 (Apr. 1996); U.S. Patent No. 5,491,644; R. Skidmore et al., *A Comprehensive In-Building and Microcellular Wireless Communication System Design Tool*, The Bradley Department of Electrical Engineering, MPRG-TR-97-13 (Jun. 1997); U.S. Patent No. 5,987,328; Robert Morrow et al., *Getting In*, Wireless Review, Vol. 17, No. 5 (Mar. 1, 2000); (iii) S. Fortune, et al., *WISE Design of Indoor Wireless Systems: Practical Computation and Optimization*, IEEE Computational Science & Engineering, at pp. 58-68 (Spring, 1995), at pp. 58-68 (mentioned in the background section of U.S. Patent No. 7,055,107, another Rappaport and Skidmore patent filed just days before the filing date of the ‘454 patent by the same attorneys that filed the ‘454 patent); and (iv) the following additional publications authored, at least in part, by Theodore Rappaport: Theodore Rappaport et al., *Curriculum Innovation for Simulation and Design of Wireless Communications Systems*, ASEE Annual Conference Proceedings (1996); Keith Blankenship et al., *Measurements and Simulation of Radio Frequency Impulsive Noise in Hospitals and Clinics*, Proceedings of the 47th IEEE Vehicular Technology (1997); Donna

Krizman et al., *Modeling and Simulation of Narrowband Phase from the Wideband Channel Impulse Response*, Proceedings of the 47th IEEE Vehicular Technology (1997); Hanif Sherali et al., *Optimal Location of Transmitters for Micro-Cellular Radio Communication System Design*, IEEE Journal on Selected Areas in Communications, Vol. 14, No. 4 (May 1996); Lynn Abbott et al., *Interactive Computation of Coverage Regions for Indoor Wireless Communication*, Proceedings of SPIE - The International Society for Optical Engineering (1995); Jorgen Andersen et al., *Propagation Measurements and Models for Wireless Communications Channels*, IEEE Communications Magazine, Vol. 33, No. 1 (Jan. 1995); M. Panjwani et al., *An Interactive System for Visualizing Wireless Communication Coverage within Buildings*, Wireless Personal Communications, Virginia Tech's 4th Symposium (June 1-3, 1994); and Theodore Rappaport, *Sponsored Research in Radio Propagation and System Design Final Report* (Sep. 26th, 1997).

59. Aruba is informed and believes, and on that basis alleges, that individuals charged with a duty of candor on behalf of Wireless Valley failed, with an intent to deceive, to disclose to the U.S. Patent and Trademark Office the SitePlanner 3.0 product and 1998 manual describing that product. On information and belief, Wireless Valley offered for sale and sold this product and published this manual at least two years before the '454 patent was filed. Wireless Valley has stated in motion papers filed before the Court that the SitePlanner 3.0 product is "in all material respects the same" as a later version of the same product, SitePlanner 3.16, that Wireless Valley recognized was material and attempted, unsuccessfully, to disclose to the Patent Office. Two of the three inventors of the '454 patent were listed on the SitePlanner 3.0 manual. In addition, on information and belief, the representatives of Wireless Valley who attempted to disclose the SitePlanner 3.16 product to the Patent Office knew about the SitePlanner 3.0 product and product manual. All of these individuals knew or should have known that the 3.0 product and product manual were material to patentability, and, on information and belief, withheld them from the patent office with intent to deceive.

60. In light of the above, the '454 patent is not enforceable due to inequitable conduct.

NINTH DEFENSE – INEQUITABLE CONDUCT ('622 PATENT)

61. Aruba is informed and believes, and on that basis alleges, that individuals charged with a duty of candor on behalf of Wireless Valley failed, with an intent to deceive, to properly disclose to the U.S. Patent and Trademark Office information material to the patentablity of the '622 patent and failed to follow the requirements of the Manual of Patent Examining Procedure necessary to have this information considered by the U.S. Patent and Trademark Office, and made false and misleading statements to the U.S. Patent and Trademark Office during the prosecution of the '622 patent.

62. This information includes, but is not limited to, U.S. Patent No. 6,505,045 (the "'045 patent"). At the relevant time, the Manual of Patent Examining Procedure stated that "It is desirable to avoid the submission of long lists of documents if it can be avoided. Eliminate clearly irrelevant and marginally pertinent cumulative information. ***If a long list is submitted, highlight those documents which*** have been specifically brought to applicant's attention and/or ***are known to be of most significance.***" Despite the highly material disclosure of the '045 patent, individuals charged with a duty of candor on behalf of Wireless Valley cited the reference by including it as reference number 98 in an Information Disclosure Statement that included a long list of many complex separate documents, all submitted at the same time, to increase the chance that the '045 patent would be overlooked by the patent examiner, and stated that the '045 patent was "only cited as constituting related art of which the applicant is aware" and specifically disclaimed that "the references are relevant or material to the claims."

63. Aruba is informed and believes, and on that basis alleges, that individuals charged with a duty of candor on behalf of Wireless Valley failed, with an intent to deceive, to disclose to the U.S. Patent and Trademark Office the SitePlanner 3.0 product and 1998 manual describing that product. On information and belief, Wireless Valley offered for sale and sold this product and published this manual at least two years before the earliest possible priority date for any

claim of the '622 patent. Wireless Valley has stated in motion papers filed before the Court that the SitePlanner 3.0 product is "in all material respects the same" as a later version of the same product, SitePlanner 3.16, that Wireless Valley recognized was material and attempted to disclose to the Patent Office. Wireless Valley failed to provide a complete copy of the 3.16 manual to the Patent Office, however, but instead excised numerous pages of the document that contain information that the examiner would have found material to patentability of the claims. Two of the three inventors of the '622 patent were listed on the SitePlanner 3.0 manual. In addition, on information and belief, the representatives of Wireless Valley who provided the excerpts of the SitePlanner 3.16 manual to the Patent Office knew about the SitePlanner 3.0 product and product manual. All of these individuals knew or should have known that the 3.0 product and product manual were material to patentability, and, on information and belief, withheld them from the ~~patent office~~Patent Office with intent to deceive.

64. In light of the above, the '622 patent is not enforceable due to inequitable conduct.

TENTH DEFENSE – UNCLEAN HANDS

65. Aruba incorporates the allegations of Paragraphs 42 through 64 here.

66. By reason of the acts alleged above, as incorporated, each of Symbol and Wireless Valley are barred from recovery for any asserted infringement of the patents-in-suit by the equitable doctrine of unclean hands.

ELEVENTH DEFENSE – PROSECUTION HISTORY ESTOPPEL

67. Symbol and Wireless are estopped from construing the asserted claims of the patents-in-suit to read on Symbol's products or processes by reasons of statements made to the U.S. Patent and Trademark Office during the prosecution of the applications that led to the issuance of the patents-in-suit.

TWELFTH DEFENSE – PLAINTIFFS' FAILURE TO GIVE NOTICE

68. To the extent Symbol and Wireless Valley seek damages for alleged infringement prior to its giving actual or constructive notice of the patents-in-suit patent to Aruba, the relief they seek is barred by 35 U.S.C. § 287.

DEMAND FOR A JURY TRIAL

69. Aruba requests a trial by jury on all issues so triable.

DENIAL OF PLAINTIFFS' PRAYER FOR RELIEF

70. Aruba denies that Symbol or Wireless Valley are entitled to an award of any relief at all or the relief sought in their prayer for relief against Aruba. Aruba has not infringed, directly, indirectly, contributorily or by inducement, literally or equivalently, willfully or otherwise, any of the asserted claims of the patents-in-suit. Symbol's and Wireless Valley's prayer should be denied its entirety and with prejudice, and Symbol and Wireless Valley should take nothing.

COUNTERCLAIMS

THE PARTIES

71. Aruba is a corporation organized under the laws of the State of Delaware with its principal place of business at 1322 Crossman Avenue, Sunnyvale, California 94089-1113. Aruba was founded in 2002 and went public in 2007. Aruba delivers an enterprise mobility solution that enables secure access to data, voice and video applications across wireless and wireline enterprise networks. It has won many, many awards for its technology innovations.

72. According to the Complaint, Symbol is a corporation organized under the laws of the State of Delaware, with its principal place of business at One Motorola Plaza, Holtsville New York 11742-1300. According to filings with the U.S. Securities and Exchanges Commission, Symbol is a wholly-owned subsidiary of global behemoth Motorola, Inc., and was acquired by Motorola in September 2006.

73. According to the Complaint, Wireless Valley is a corporation organized under the laws of the State of Delaware with its principal place of business at 4515 Seton Center Parkway,

Suite 300, Austin, Texas 78759. According to filings with the U.S. Securities and Exchanges Commission, Wireless Valley is a wholly-owned subsidiary of global behemoth Motorola, Inc., and was acquired by Motorola in December 2005.

74. On information and belief, Motorola, Inc. is a corporation organized under the laws of the State of Delaware with its principal place of business at 1303 East Algonquin Road, Schaumburg, Illinois 60196.

75. On information and belief Motorola, Symbol, and Wireless Valley design, manufacture, and sell in the United States wireless switches, access points and other components for use in connection with WLANs, as well as software for monitoring, and managing WLANs.

JURISDICTION AND VENUE

76. ~~74.~~ This Court has subject-matter jurisdiction over Aruba's patent counterclaims, which arise under the patent laws of the United States, pursuant to 28 U.S.C. §§ 1331, 1338, 2201, and 2202.

77. ~~75.~~ This Court has personal jurisdiction over Symbol, at least because Symbol filed its Complaint for patent infringement in this Court, in response to which these counterclaims are filed. Personal jurisdiction is also proper in this Court because, upon information and belief, Symbol, among other things, places its infringing products in the stream of commerce, which stream is directed at this district.

78. ~~76.~~ This Court has personal jurisdiction over Wireless Valley, at least because Wireless Valley filed its Complaint for patent infringement in this Court, in response to which these counterclaims are filed. Personal jurisdiction is also proper in this Court because, upon information and belief, Wireless Valley, among other things, places its infringing products in the stream of commerce, which stream is directed at this district.

79. This Court has personal jurisdiction over Motorola, Inc., because Motorola is a Delaware corporation with an agent for service of process in Delaware. Personal jurisdiction is also proper in this Court because, upon information and belief, Motorola, among other things, places its infringing products in the stream of commerce, which stream is directed at this district.

80. ~~77.~~ Venue is established in this district for Motorola, Symbol and Wireless Valley pursuant to 28 U.S.C. § 1391 and 1400. Venue is also established in this Court ~~because~~for Symbol and Wireless Valley because they have consented to the propriety of venue in this Court by filing their respective claims for patent infringement in this Court, in response to which Aruba files these counterclaims.

COUNT 1

DECLARATORY JUDGMENT OF NON-INFRINGEMENT

('922 AND '923 PATENTS)

81. ~~78.~~ Aruba incorporates Paragraphs 1 through 68 and 71 through ~~77~~80 here.

82. ~~79.~~ An actual and justiciable controversy exists between Aruba and Symbol with respect to the asserted claims of the '922 and '923 patents because Symbol has brought this action against Aruba alleging that Aruba infringes claims of the '922 and '923 patents, which allegation Aruba denies. Absent a declaration of noninfringement, Symbol will continue wrongfully to assert claims of the '922 and '923 patents against Aruba, and thereby cause Aruba irreparable injury and damage.

83. ~~80.~~ Aruba has not infringed, and does not infringe, the asserted claims of the '922 or '923 patents, either directly or indirectly, literally or under the doctrine of equivalents, willfully, or otherwise, and Aruba is entitled to a declaration to that effect.

COUNT 2

DECLARATORY JUDGMENT OF INVALIDITY

('922 AND '923 PATENTS)

84. ~~81.~~ Aruba incorporates Paragraphs 1 through 68 and 71 through ~~77~~83 here.

85. ~~82.~~ An actual and justiciable controversy exists between Aruba and Symbol with respect to the asserted claims of the '922 and '923 patents because Symbol has brought this action against Aruba alleging that the asserted claims of the '922 and '923 patents are valid, which allegation Aruba denies. Absent a declaration of invalidity, Symbol will continue

wrongfully to assert claims of the '922 and '923 patents against Aruba, and thereby cause Aruba irreparable injury and damage.

86. ~~83.~~ The '922 and '923 patents are invalid for failure to comply with the requirements of Title 35, United States Code, including but not limited to §§ 101, 102, 103, and/or 112, and Aruba is entitled to a declaration to that effect.

COUNT 3

DECLARATORY JUDGMENT OF UNENFORCEABILITY

('922 AND '923 PATENTS)

87. ~~84.~~ Aruba incorporates Paragraphs 1 through 68 and 71 through ~~77~~86 here.

88. ~~85.~~ An actual and justiciable controversy exists between Aruba and Symbol with respect to the asserted claims of the '922 and '923 patents because Symbol has brought this action against Aruba alleging that the asserted claims of the '922 and '923 patents are enforceable, which allegation Aruba denies. Absent a declaration of unenforceability, Symbol will continue wrongfully to assert claims of the '922 and '923 patents against Aruba, and thereby cause Aruba irreparable injury and damage.

89. ~~86.~~ As set forth above, one or more people substantively involved in the prosecution of the application leading to the '922 and '923 patents were aware of information material to the patentability of the claims of the '922 and '923 patents, but withheld that information from the U.S. Patent and Trademark Office with the intent to deceive, during the prosecution of the '922 and '923 patents.

90. ~~87.~~ In light of the above, the '922 and '923 patents are not enforceable due to inequitable conduct.

COUNT 4

DECLARATORY JUDGMENT OF NON-INFRINGEMENT

('454 AND '622 PATENTS)

91. ~~88.~~ Aruba incorporates Paragraphs 1 through 68 and 71 through ~~77~~90 here.

92. ~~89.~~ An actual and justiciable controversy exists between Aruba and Wireless Valley with respect to the asserted claims of the ’454 and ’622 patents because Wireless Valley has brought this action against Aruba alleging that Aruba infringes claims of the ’454 and ’622 patents, which allegation Aruba denies. Absent a declaration of noninfringement, Wireless Valley will continue wrongfully to assert claims of the ’454 and ’622 patents against Aruba, and thereby cause Aruba irreparable injury and damage.

93. ~~90.~~ Aruba has not infringed, and does not infringe, the asserted claims of the ’454 and ’622 patents, either directly or indirectly, literally or under the doctrine of equivalents, willfully, or otherwise, and Aruba is entitled to a declaration to that effect.

COUNT 5

DECLARATORY JUDGMENT OF INVALIDITY

(’454 AND ’622 PATENTS)

94. ~~91.~~ Aruba incorporates Paragraphs 1 through 68 and 71 through ~~77~~91 here.

95. ~~92.~~ An actual and justiciable controversy exists between Aruba and Wireless Valley with respect to the asserted claims of the ’454 and ’622 patents because Wireless Valley has brought this action against Aruba alleging that the asserted claims of the ’454 and ’622 patents are valid, which allegation Aruba denies. Absent a declaration of invalidity, Wireless Valley will continue wrongfully to assert claims of the ’454 and ’622 patents against Aruba, and thereby cause Aruba irreparable injury and damage.

96. ~~93.~~ The ’454 and ’622 patents are invalid for failure to comply with the requirements of Title 35, United States Code, including but not limited to §§ 101, 102, 103, and/or 112, and Aruba is entitled to a declaration to that effect.

COUNT 6

DECLARATORY JUDGMENT OF UNENFORCEABILITY

(’454 AND ’622 PATENTS)

97. ~~94.~~ Aruba incorporates Paragraphs 1 through 68 and 71 through ~~77~~96 here.

98. ~~95.~~ An actual and justiciable controversy exists between Aruba and Wireless Valley with respect to the asserted claims of the '454 and '622 patents because Wireless Valley has brought this action against Aruba alleging that the asserted claims of the '454 and '622 patents are enforceable, which allegation Aruba denies. Absent a declaration of unenforceability, Wireless Valley will continue wrongfully to assert claims of the '454 and '622 patents against Aruba, and thereby cause Aruba irreparable injury and damage.

99. ~~96.~~ As set forth above, one or more people substantively involved in the prosecution of the application leading to the '454 and '622 patents were aware of information material to the patentability of the claims of the '454 and '622 patents, but withheld that information from the U.S. Patent and Trademark Office with the intent to deceive, during the prosecution of the '454 and '622 patents. In addition, with respect to the '622 patent, and as set forth above, Aruba is informed and believes, and on that basis alleges, that individuals charged with a duty of candor on behalf of Wireless Valley made false and misleading statements to the U.S. Patent and Trademark Office during the prosecution of the '622 patent.

100. ~~97.~~ In light of the above, the '454 and '622 patents are not enforceable due to inequitable conduct.

COUNT 7

INFRINGEMENT OF THE '524 PATENT

101. Aruba incorporates Paragraphs 1 through 68 and 71 through 100 here.

102. Aruba is the sole owner of United States Patent No. 7,295,524 ("the '524 Patent"), entitled "Methods, Apparatuses and Systems Facilitating Management of Airspace in Wireless Computer Network Environments," duly and legally issued by the Patent Office on November 13, 2007 to Gordon Paul Gray, Jason Edward Luther, and Daniel Thomas Augustine. A copy of the '524 Patent is attached hereto as Exhibit A.

103. On information and belief, Motorola, Symbol, and Wireless Valley have been and currently are infringing, contributing to the infringement of, and/or inducing the infringement of the '524 Patent by, among other things, making, using, selling, offering to sell, and/or importing

within the territorial boundaries of the United States, products and services—including but not limited to, wireless switches, access points, and other hardware and software for use in connection with wireless networks that operate to perform rogue device detection—that are covered by one or more claims of the '524 Patent.

104. On information and belief, Motorola's, Symbol's, and Wireless Valley's infringement of the '524 Patent has been and is willful, and will continue unless enjoined by this Court. Aruba has suffered, and will continue to suffer, irreparable injury as a result of this willful infringement. Pursuant to 35 U.S.C. § 284, Aruba is entitled to damages for infringement and treble damages. Pursuant to 35 U.S.C. § 283, Aruba is entitled to a permanent injunction against further infringement.

105. This case is exceptional and, therefore, Aruba is entitled to attorneys' fees pursuant to 35 U.S.C. § 285.

COUNT 8

INFRINGEMENT OF THE '113 PATENT

106. Aruba incorporates Paragraphs 1 through 68 and 71 through 105 here.

107. Aruba is the sole owner of United States Patent No. 7,376,113 ("the '113 Patent"), entitled "Mechanism for Securely Extending A Private Network," duly and legally issued by the Patent Office on November 13, 2007 to John Richard Taylor, Pradeep J. Iyer, and Randy Chou. A copy of the '113 Patent is attached hereto as Exhibit B.

108. On information and belief, Motorola, Symbol, and Wireless Valley have been and currently are infringing, contributing to the infringement of, and/or inducing the infringement of the '113 Patent by, among other things, making, using, selling, offering to sell, and/or importing within the territorial boundaries of the United States, products and services—including but not limited to, wireless switches, access points, and other hardware and software for use in connection with wireless networks that operate to securely extend networks—that are covered by one or more claims of the '113 Patent.

109. On information and belief, Motorola's, Symbol's and Wireless Valley's infringement of the '113 Patent has been and is willful, and will continue unless enjoined by this Court. Aruba has suffered, and will continue to suffer, irreparable injury as a result of this willful infringement. Pursuant to 35 U.S.C. § 284, Aruba is entitled to damages for infringement and treble damages. Pursuant to 35 U.S.C. § 283, Aruba is entitled to a permanent injunction against further infringement.

110. This case is exceptional and, therefore, Aruba is entitled to attorneys' fees pursuant to 35 U.S.C. § 285.

DEMAND FOR A JURY TRIAL

111. ~~98.~~ Aruba requests a trial by jury on all issues so triable.

PRAYER FOR RELIEF

WHEREFORE, Aruba prays the Court as follows:

A. That the Court enter judgment for Aruba against each of Symbol and Wireless Valley on their Complaint;

B. That each of Symbol and Wireless Valley take nothing by their Complaint;

C. That the Court dismiss each of Symbol's and Wireless Valley's claims with prejudice;

D. That the Court declare each and every asserted claim of the '922, '923, '454 and '622 patents to be (a) not infringed by Aruba, (b) invalid, and (c) unenforceable;

E. That, under 35 U.S.C. § 285, the Court deem this to be an exceptional case ~~based on the conduct of each of Symbol and Wireless Valley in commencing and pursuing this action,~~ and that the Court award Aruba its "reasonable attorney fees" against each of Motorola, Symbol~~,~~ and Wireless Valley;

F. That the Court award Aruba its costs of suit;~~and~~

G. That Motorola, Symbol and Wireless Valley be adjudged to have infringed the '524 Patent and/or the '113 Patent;

H. That Motorola, Symbol and Wireless Valley, their agents, employees, representatives, successors and assigns, and those persons in active concert or participation with any of them, and their successors and assigns be permanently enjoined from infringement, inducement of infringement, and contributory infringement of the '524 Patent and/or '113 Patent, including but not limited to making, using, offering for sale, selling and importing into the United States any devices or products that infringe the '524 Patent and/or '113 Patent;

I. That Motorola, Symbol and Wireless Valley be adjudged to have willfully infringed the '524 Patent and/or the '113 Patent, and that continued infringement by Motorola, Symbol and Wireless Valley is willful;

J. That the Court award Aruba damages in an amount adequate to compensate for the infringement by Motorola, Symbol and Wireless Valley of the '524 Patent and/or '113 Patent, but in no event less than a reasonable royalty under 35 U.S.C. § 284;

K. That the Court enter an order trebling any and all damages awarded to Aruba by reason of willful infringement by Motorola, Symbol and Wireless Valley of the '524 Patent and/or '113 Patent under 35 U.S.C. § 284;

L. That the Court enter an order awarding Aruba interest on the damages awarded and its costs under 35 U.S.C. § 284; and

M. That the Court award Aruba such other and additional relief as this Court deems just and proper.

/s/ Frederick L. Cottrell,
III

Of Counsel:

MATTHEW D. POWERS
~~VERNON M. WINTERS~~
~~BRANDON C. CONARD~~
WEIL, GOTSHAL & MANGES LLP
Silicon Valley Office
201 Redwood Shores Parkway
Redwood Shores, CA 94065
Telephone: (650) 802-3000

NICHOLAS GROOMBRIDGE
PAUL E. TORCHIA
ETAI LAHAV
WEIL, GOTSHAL & MANGES LLP
New York Office
767 Fifth Avenue
New York, NY 10153-0119
Telephone: (212) 310-8000

Dated: ~~June 3,~~July 16, 2008

Frederick L. Cottrell, III (#2555)
Richards, Layton & Finger
One Rodney Square
920 North King Street
P. O. Box 551
Wilmington, DE 19899
Telephone: (302) 651-7700
cottrell@rlf.com

Attorneys for Defendant and Counter-Claimant
ARUBA NETWORKS, INC.

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF DELAWARE

SYMBOL TECHNOLOGIES, INC., a Delaware Corporation, and WIRELESS VALLEY COMMUNICATIONS, INC., a Delaware Corporation,

Plaintiffs,

v.

ARUBA NETWORKS, INC., a Delaware Corporation,

Defendant.

ARUBA NETWORKS, INC., a Delaware Corporation

Counter-Claim Plaintiff,

v.

MOTOROLA, INC., a Delaware Corporation, SYMBOL TECHNOLOGIES, INC., a Delaware Corporation, and WIRELESS VALLEY COMMUNICATIONS, INC., a Delaware Corporation,

Counter-Claim Defendants.

ORDER

C. A. No. 07-519-JJF

WHEREAS, the Court having considered the Motion of Defendant Aruba Networks, Inc. ("Aruba") to file an amended answer and counterclaims and join Motorola, Inc. as counterclaim defendant;

IT IS HEREBY ORDERED this ______ day of _______________, 2008 that the Motion is GRANTED in its entirety and that Aruba is permitted to file and serve its amended pleading on Symbol Technologies, Inc. ("Symbol"), Wireless Valley, Inc. ("Wireless Valley"), and Motorola, Inc. ("Motorola") in the form attached as Exhibit A to the Motion. The amended pleading is to be deemed filed against Symbol, Wireless Valley, and Motorola on the date of this Order. The amended pleading is to be deemed served against Symbol and Wireless Valley on the date of this Order.

IT IS FURTHER ORDERED that the case caption used above shall be the caption used henceforth by the parties in this action.

____
United States District Judge

CERTIFICATION PURSUANT TO DISTRICT OF DELAWARE LOCAL RULE 7.1.1

Counsel for Aruba Networks, Inc. has made a reasonable effort to reach agreement with Plaintiffs' counsel pursuant to District of Delaware Local Rule 7.1.1. The parties were unable to reach agreement.

/s/ Frederick L. Cottrell, III
Frederick L. Cottrell, III (#2555)
Richards, Layton & Finger
One Rodney Square
920 North King Street
P. O. Box 551
Wilmington, DE 19899
Telephone: (302) 651-7700

Attorneys for Defendant and Counter-Claimant
ARUBA NETWORKS, INC.

OF COUNSEL:

MATTHEW D. POWERS
WEIL, GOTSHAL & MANGES LLP
Silicon Valley Office
201 Redwood Shores Parkway
Redwood Shores, CA 94065
Telephone: (650) 802-3000

NICHOLAS GROOMBRIDGE
PAUL E. TORCHIA
ETAI LAHAV
WEIL, GOTSHAL & MANGES LLP
New York Office
767 Fifth Avenue
New York, NY 10153-0119
Telephone: (212) 310-8000

Dated: July 16, 2008